VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

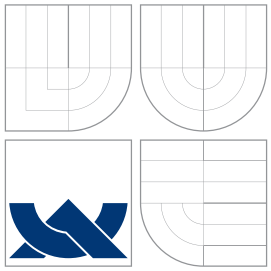
ZABEZPEČOVACÍ SYSTÉM PRO DOMÁCNOST S VYUŽITÍM GSM KOMUNIKACE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

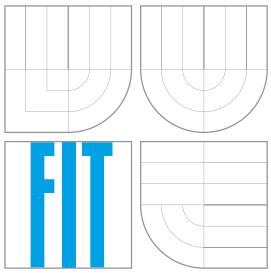
AUTOR PRÁCE
AUTHOR

TOMÁŠ KŘESAL

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

ZABEZPEČOVACÍ SYSTÉM PRO DOMÁCNOST S VYUŽITÍM GSM KOMUNIKACE

GUARD SYSTEM FOR HOUSEHOLD WITH USAGE OF GSM COMMUNICATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — TOMÁŠ KŘESAL
AUTHOR

VEDOUCÍ PRÁCE — Ing. JOSEF HÁJEK
SUPERVISOR

BRNO 2010

Abstrakt

Tato práce je věnovaná problematice zabezpečení domácností. Diskutuje současné metody ochrany, jejich typické vlastnosti a nedostatky. Na základě získaných informací z úvodních kapitol je navržen a zkonstruován zabezpečovací systém pro domácnost s přenosem poplachu na mobilní telefon. Vzdálené ovládání elektrických spotřebičů a dohled na domácnost prostřednictvím internetu rozšiřuje použitelnost celého systému.

Hardwarové realizaci navrženého zařízení je věnován závěr této práce. Softwarová realizace není v této práci probírána a bude součástí dalšího vývoje.

Abstract

Theme of the Bachelor's thesis is the issue of security of households. Discusses the current methods of protection, of their typical characteristics and shortcomings. Based on information gathered from the opening chapters is designed and engineered an electronic security device with alarm transmission to the mobile phone. Remote control of electrical appliances and supervision households via the Internet extends the applicability of the system.

The conclusion of this work is devoted to the hardware implementation of the proposed security system. Software implementation is not discussed here and will be part of further development.

Klíčová slova

Elektronický zabezpečovací systém, EZS, Mobilní telefon, GSM, ZigBee, Ethernet, RFID, USB, ATxMega, Inteligentní domácnost, UPS, Záložní zdroj

Keywords

Electronic security system, Cell phone, Mobile phone, GSM, ZigBee, Ethernet, RFID, USB, ATxMega, Smart household, UPS

Citace

Tomáš Křesal: Zabezpečovací systém pro domácnost s využitím GSM komunikace, bakalářská práce, Brno, FIT VUT v Brně, 2010

Zabezpečovací systém pro domácnost s využitím GSM komunikace

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Josefa Hájka.

.....
Tomáš Křesal
17. května 2010

Poděkování

Tímto bych velmi rád poděkoval vedoucímu práce Ing. Josefu Hájkovi za jeho velice vstřícné jednání a odbornou pomoc při návrhu zabezpečovacího systému. Dále obrovské poděkování patří Doc. Ing., Dipl.-Ing. Martinovi Drahanskému, Ph.D., který svými odbornými znalostmi přispěl k vytvoření výsledného zařízení a zajistil finanční prostředky pro jeho realizaci.

Obsah

Kapitola 1

Úvod

Žijeme v moderní společnosti a jsme obklopeni rychle se rozvíjející technikou. Dnes téměř každý vlastní nejméně jeden mobilní telefon. Byť dodržujeme psaná i nepsaná pravidla slušného chování, často se najdou lidé, kteří nám rádi ublíží. Dostáváme se do situace, kdy musíme začít myslet na bezpečí nejen své, ale i celé rodiny.

Vždy mě bavilo rozebírat různá elektronická zařízení. Byl jsem okouzlen krásou stále se zmenšujících integrovaných obvodů. Až jednoho dne jsem začal také podobná zařízení sám konstruovat. Mimo jiné se zabývám i sebeobranou a tak jsem začal myslet také na bezpečí vlastního majetku. Propojením těchto dvou oborů se zrodila myšlenka navrhnout užitečné zařízení zvyšující pocit bezpečí v místě našeho domova.

Ze statistik z roku 2008 vyplývá, že se stále mírně zvyšuje majetková trestná činnost provedená vloupáním do bytů a rodinných domů. Ročně je zaznamenáno téměř deset tisíc takových případů s celkovou škodou přesahující 500 mil. Kč. Bohužel pouze přibližně 5% obyvatel má své domácnosti vybavené elektronickým zabezpečovacím systémem (dále jen „EZS“). Tato skutečnost velmi komplikuje práci Policie ČR, což se projevuje urputně nízkou objasněností pohybující se kolem 19% ([21], [38]).

Každý z nás má ve své domácnosti něco cenného. Ať už se jedná o finance, elektrospotřebiče nebo šperky, všechny nás spojuje jedna společná věc. Pocit bezpečí a soukromí. Je mi opravdu velmi líto lidí, kteří byli vykradeni a tentýž den se odebrali v tomtéž bytě ke spánku. Jistě mi dáte za pravdu, že spánek to nemůže být nikterak klidný, nýbrž plný nervů a pocitu, že se zloděj může vrátit.

Tato práce se zabývá komplexním návrhem EZS, který v reálném čase bude oznamovat bezpečnostní hrozbu v místě nemovitosti (například sirénou) a zároveň bude přenášet poplach na mobilní telefon případně pult centrální ochrany. Navržený EZS je určen pro zabezpečení od malých bytů až po rozlehlé rodinné domy. Není vyloučeno jeho použití v obchodech, restauracích nebo víkendových chatách apod. Dále bude zařízení dostupné pro širokou veřejnost a v neposlední řadě nabídne komfort, kterým se chlubí profesionální výrobky firem Jablotron [15] nebo Paradox [26], například domovní automatizace.

V následujícím textu bude popsán hardwarový návrh a konstrukce záložního zdroje, GSM modulu, řídící jednotky s rozhraním Ethernet pro sítě TCP/IP, modulu klávesnice sloužící i jako čtečka pro bezkontaktní identifikaci postavené na technologii RFID a pro rozšíření počtu připojitelných čidel modul vstupů a výstupů.

Doufám, že i budoucí studenti naleznou v této práci poučení a inspiraci pro konstrukci vlastních EZS nebo využijí rozsáhlé možnosti celého zařízení a budou se stejně jako já zabývat jeho dalším vývojem.

Kapitola 2

Způsoby zabezpečení a střežení objektů

Tato kapitola čtenáře seznámí s důvody proč zabezpečit nemovitost a se základním rozdělením typů jejich zabezpečení a střežení. Rozebírá typické vlastnosti bezpečnostních prvků a poukazuje na jejich nedostatky.

2.1 Proč zabezpečit nemovitost?

Každé zabezpečení, o kterém je případný narušitel informován působí preventivním dojmem. Myšlení narušitele je snadno pochopitelné. S minimálním úsilím získat maximální zisk. Každá překážka zvyšující možnost odhalení nebo chycení činí jeho práci složitější a zvyšuje jeho psychické vypětí. Většinou jde zloděj takzvaně „na slepo“ a nemá přesnou představu, co v bytě nalezne. Proto mu téměř nezáleží na tom, který byt se rozhodne vykrást. Rozhoduje se zejména podle rizika odhalení.

Můžeme se setkat s myšlenkou, že je dobré narušitele neinformovat o našem zabezpečení a spolehnout se tak na moment překvapení. Tehdy doufáme, že se narušitel vyleká a zanechá svého protiprávního jednání. Souhlasím. Určitě je na tom hodně pravdy. Řekněme však, že narušitel očekával snadnou práci a po chvíli, co vstoupil do objektu, se bez varování rozezněl alarm. Každý z nás se rozzlobí, když se mu něco nepovede. Někdo situaci okoření patřičnou poznámkou, jiný pěstí udeří do stolu nebo klávesnice. I zloděj takto může reagovat. Může se však rozzuřit až do nepříčetnosti a začít vandalizovat náš majetek. Chraň bůh, aby ho ještě v tento moment někdo vyrušil. Situace může dopadnout katastrofálně.

Narušitel může po takovém překvapení nemovitost dle našich záměrů urychleně opustit. Avšak není v našich silách mu zabránit, aby přišel znovu a nechtěl se nám například žhářským útokem pomstít. Vím, jedná se o extrémní situaci. Ale pokud chceme nemovitost zabezpečit, musíme zvážit i toto hledisko. Osobně proto doporučuji informovat například nápisem: „Objekt je střežen elektronickým a kamerovým zabezpečovacím systémem.“ Případně nápis doplnit vhodným výstražným obrázkem. Například obrázek 2.1.

Z výše uvedeného nepřímo vyplývá, že s rostoucím počtem zabezpečených objektů roste riziko objektů nezabezpečených. Člověk by se měl zamyslet i nad touto situací a dle filmového vzoru „Zítra to roztočíme, drahoušku…!“ se snažit mít kvalitnější zabezpečení než má jeho soused.

Rozhodneme-li se zabezpečit nemovitost, musíme posuzovat druh a způsob jejího využití. Budeme postupovat odlišně při zabezpečení malého bytu nebo velkého rodinného

Obrázek 2.1: Výstražná cedule

domu. V dalším textu se krátce seznámíme s dostupnými typy zabezpečení.

2.2 Mechanické zábranné systémy

Tato podkapitola byla volně převzata z [36].

Mechanické zábranné systémy (užívá se zkratka MZS) patří mezi nejstarší bezpečnostní prostředky. Dlouho před objevením elektřiny měli lidé potřebu chránit svůj život a později také majetek. K těmto účelům využívali dostupné materiály, z počátku kámen a především dřevo. Vyráběly se závory a petlice. Chránily se vstupní a okenní prostory. Stavěly se příkopy, hradby a padací mosty. Zásadní zlom ve vývoji nastal s příchodem zámkařské techniky v dobách řecké a římské kultury. V 19. století začal masivní rozvoj tohoto oboru, na který v dnešní době navazujeme použitím moderních elektronických zařízení.

MZS jsou konstruovány tak, aby narušitele při jejich překonávání zdrželi co nejdéle. Ideálně do doby, kdy je možné provést proti narušiteli fyzický zákrok. Nutno vyvrátit marketingové tvrzení o nepřekonatelnosti některých zařízení. Je třeba mít na paměti, že všechny MZS jsou v konečném čase překonatelné a právě doba jejich překonávání závisí na několika dílčích faktorech. Zejména útočníkova dobrá znalost bezpečnostní konstrukce a kvalitní použité nástroje tento čas velmi snižují. Obecně je doporučeno nenechávat na svém pozemku žádný nástroj, který by mohl útočníkovi pomoci k vniknutí do objektu. Stejně tak nenabídnout možnost využít elektrickou zásuvku. Bohužel rozvoj techniky pomáhá také útočníkům, kteří mohou využít elektrická zařízení napájená z akumulátorů. Což ve výsledku klade vyšší nároky na kvalitu MZS a materiálů z nichž jsou vyráběny.

Ochrana pomocí mechanických prvků je velice rozsáhlá a můžeme ji proto rozdělit do tří základních kategorií. Prostředky obvodové, objektové a individuální ochrany.

2.2.1 Prostředky obvodové ochrany

Jedná se o mechanické zábrany, které nejsou přímou součástí vlastního objektu. Nejčastěji bývají umístěny na hranici pozemku a brání volnému vstupu na něj. Patří zde zejména ochranné zdi a ploty využívající dalších prvků jako jsou dveře, vrata a branky. Případnému útočníkovi musí tyto zábrany znesnadnit nebo zcela zamezit jejich překonání včetně přelezení nebo podlezení. Proti přelezení se využívá vrcholové ochrany spočívající v instalaci ostnatého nebo žiletkového drátu na vrcholu zdi či plotu.

Nezabezpečujeme-li zrovna věznici nebo armádní objekt musíme zvažovat i vzhled těchto bezpečnostních prvků. Desetimetrová masivní zeď se bude jistě hůře překonávat než dvoumetrová. Na druhou stranu i hůře vypadá. Z hlediska bezpečnosti rodinného domu je vhodné, aby bylo vidět na náš pozemek i z přilehlého okolí (například od sousedů). K tomuto účelu se nabízí použít plot z kovových profilů, který je průhledný, splňuje bezpečnostní požadavky a je vyráběn v mnoha designových provedeních, viz obrázek 2.2.

Obrázek 2.2: Plot s kovovým profilem [25]

2.2.2 Prostředky objektové ochrany

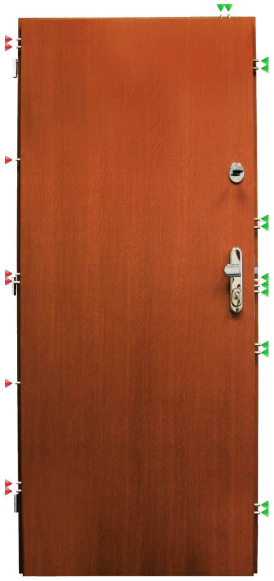
Každý dům nebo byt má několik stavebních otvorů, které mohou útočníkovi sloužit jako vstup do objektu. Jsou jimi prostory dveří, oken, balkónových oken, vikýřů, zásobovacích šachet apod. Pro jejich zabezpečení slouží skupina prvků objektové ochrany. Vysoký důraz je kladen na kvalitu hlavních vstupních dveří. Většina pachatelů právě toto místo využívá pro vstup do objektu. Po neúspěchu u dveří zkouší využít okna v přízemí. Popíšeme si tato dvě kritická místa podrobněji.

Bezpečnostní dveře odolné proti vloupání musí splňovat nemálo kritérií. Musí být odolné proti proražení, vypáčení nebo vysazení ze závěsu. Jejich konstrukce může být různá. Nejčastěji sendvičová s kovovým zesíleným rámem a protipožární nebo neprůstřelnou výplní. Musí být zavěšeny nejméně na třech místech a mít rozšířený počet uzamykacích a zajišťujících míst po celém obvodu dveřního křídla, viz obrázek 2.3a. Vhodné jsou nejméně dva uzamykací zámky.

Právě zámek je vysoce důležitou částí každého zabezpečení nemovitého objektu. Nejznámější a nejpoužívanější je cylindrická vložka, která má své počátky už ve starém Egyptě. Dnešní podobu jí dal Linus Yale v roce 1865. Navzdory jejímu stáří se tento koncept nadále vyvíjí a s dostupnými novými technologiemi i zlepšuje. Špičkou v tomto oboru jsou cylindrické vložky vybavené elektronikou. Pro jejich překonání nestačí mít přesnou podobu klíče, ale i kopii čipu uvnitř klíče. Technicky je výroba falešného klíče extrémně náročná.

Ztrátu klíče v žádném případě nesmíme podcenit. Musíme si také rozmyslet, komu jej dáme. Neměli bychom opomenout bezpečí našich dětí. Malé dítě je snadno zranitelné a odcizit mu klíče nepozorovaně nebo loupežně nepatří mezi obtížné situace pro lidi, kteří se takto živí. Také obdarovat sousedy nebo příbuzné naším klíčem nemusí být rozumné, pokud mají špatně zabezpečený svůj dům či byt.

Nepřekonatelnou touhou zloděje je otevřené okno v přízemí našeho bytu. Při odchodu z domu věnujme malou chvíli pro kontrolu oken. Když nás zrovna zloděj nepřekvapí, tak přinejmenším nevinnému dešti přijde otevřené okno vhod. Při zabezpečení oken máme



(a) Bezpečnostní dveře [31]

(b) Rozbité sklo s fólií [23]

Obrázek 2.3: Bezpečnostní dveře a fólie proti rozbití skla

prakticky dvě možnosti. Jednou z nich je instalování bezpečnostních mříží a druhou použití bezpečnostní fólie. Ideální je kombinace obou. Mříže působí na první pohled preventivně, ale mohou nám vadit z estetických důvodů. Fólie se instalují na skleněnou plochu okna a v kombinaci se sklem o tloušťce 3mm zamezují jeho násilnému rozbití. Jsou čiré a bývají vybaveny ochranou před škodlivým UV zářením. Navíc chrání uživatele před pořezáním od skla při nehodě v domácnosti. Na obrázku 2.3b je možné vidět, že při pokusu o rozbití okna zůstane sklo v rámu společně se všemi střepy.

2.2.3 Prostředky individuální ochrany

Tímto termínem označujeme skupinu bezpečnostních prvků, které slouží jako konečné místo pro úschovu cenností (financí, šperků, důležitých dokumentů apod.). Typickými zástupci této skupiny jsou trezory, ale i přenosné kufry a příruční pokladny. Je vyžadován maximální stupeň bezpečnosti, a proto jsou některé výrobky odolné i proti požáru a následnému zásahu hasičů. Stabilní trezory jsou zabudovány do konstrukce budovy a také díky jejich vysoké hmotnosti je velmi obtížné jejich odcizení.

Většina trezorů je vybavena klíčovým nebo elektronickým zámkem na heslo. Je nutné si uvědomit, že heslo napsané na boční straně trezoru nebo klíč povalující se někde kolem na bezpečnosti ani trochu nepřidá. Proto je velmi důležité mít klíč dobře schovaný a hlavně jej nemít mezi ostatními klíči. Zkušený zloděj na první pohled rozezná klíč určený k trezoru a má tak věci v něm ukryté přímo na dosah. U kvalitních trezorů se můžeme setkat se dvěma zámky nebo zámkem na klíč společně s elektronickou klávesnicí pro zadání hesla. Poslední dobou se také více prosazují čtečky biometrických údajů, zejména pak čtečky otisků prstů.

2.3 Elektronické zabezpečovací systémy

Tato podkapitola byla volně převzata z [36].

Elektrotechnika se začala teprve vyvíjet, žárovka byla vynalezena o čtvrt století později. Psal se rok 1853, když si nechal v americkém státě Massachusetts patentovat první elektronický zabezpečovací systém (používá se zkratka EZS) pan Augustus R. Pope ze Somerville. Tento systém byl určený pro domácnost, spočíval v několika kontaktech na oknech a dveřích připojených k baterii a zvonku. Při otevření dveří došlo k sepnutí kontaktu a zvonek začal zvonit. O několik let později odkoupil tento patent Edwin T. Holmes, který se posléze zasloužil o velký kus vývoje v oblasti EZS. Například uvedl do provozu první pult centrální ochrany, na který připojil bohaté firmy té doby.

Do dnešního dne elektrotechnika urazila významný kus cesty. Polovodičové součástky a jejich miniaturizace vyústili až k výkonným procesorům. Stojí za povážlenou, že i tak primitivní systém jaký byl vytvořen před více než 150 lety si dnes lidé hromadně neinstalují do svých domácností a raději je nechávají absolutně nezabezpečené. V následujícím textu se proto v krátkosti seznámíme s dnešními možnostmi EZS.

2.3.1 Ústředny EZS

Jako hlavní řídící centrum, podobně jako mozek v lidském těle, slouží v zabezpečovací technice ústředna. Ta přijímá a vyhodnocuje signály z čidel, ovládá při poplachu výstupní zařízení (např. sirény a majáčky) a uživateli nabízí možnost systém zapnout nebo vypnout. Tyto vlastnosti můžeme prohlásit za absolutní minimum, které každá ústředna EZS musí nabízet. Dále může zajišťovat napájení čidel elektrickou energií nebo nabízet mechanismy pro diagnostiku celého systému.

V zásadě jsme schopni rozdělit ústředny EZS do čtyř kategorií dle způsobu připojení čidel. Jestliže připojujeme každé čidlo k právě jednomu vstupnímu obvodu, mluvíme o smyčkové ústředně. Typické jsou svoji rozsáhlou kabelovou sítí, neboť ke každému čidlu musí být připojeny nejméně dva vodiče. Často se můžeme setkat s řešením, kdy se jednotlivá čidla zapojují sériově za sebe. Ušetří se tak na použitých vodičích, ale ochudíme se o možnost rozpoznat konkrétní čidlo, z kterého vzešel poplach.

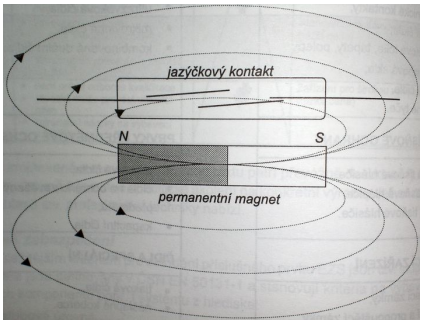
Předešlý problém řeší ústředny s přímou adresací čidel. Všechna čidla jsou připojena k datové sběrnici, po které komunikují s ústřednou. Při použití minimálního počtu vodičů (typicky čtyř, dva napájení a dva pro komunikaci) si zachováme možnost rozlišit od sebe jednotlivá čidla. Tato výhoda nám přijde vhod, když zapomeneme zavřít okno nebo nastane problém s vadným čidlem. Ovšem i tento způsob není ideální a má své omezení. Musíme brát v úvahu celkovou délku kabelového vedení a počítat s úbytky napětí na něm.

Problematika délky vedení je řešitelná s použitím opakovačů nebo specializovaných komponent. Zakopaný pes je někde jinde. Co dělat pokud chceme zabezpečit domácnost dodatečně? Provádět pracné a velmi špinavé stavební úpravy v zařízené domácnosti je zlý sen každé hospodyňky. Uložit vodiče zabezpečovacího systému do lišt na zdech je esteticky i bezpečnostně nevhodné. Řešení se skrývá v použití ústředny s bezdrátovým přenosem od čidel. Každé čidlo je samostatně adresovatelné a délku vodičů zde nemusíme řešit. Instalace takového systému je velmi snadná a stejně tak i jeho změna. Při přestěhování nábytku je přemístění čidla otázkou několika málo minut.

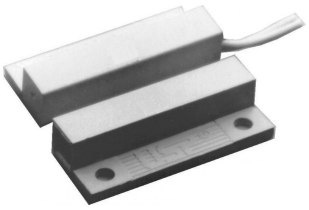
Poslední kategorií jsou ústředny smíšeného typu. Zde se kombinují vlastnosti předešle zmíněných ústředen a nabízejí tak široké možnosti využití. Zejména doplnění bezdrátových a přímo adresovatelných ústředen o smyčkové vstupy je více než vhodné. Především z ekonomických důvodů. Bezdrátová čidla nebo obecně čidla vybavená dodatečnou elektronikou jsou bezesporu nákladnější na výrobu a jejich cena se zajisté promítne u koncového zákazníka.

2.3.2 Prvky plášťové ochrany

K ochraně prostor, kterými je možné vstoupit do objektu, slouží skupina čidel nazvaná prvky plášťové ochrany. Nejčastěji se setkáváme s magnetickými kontakty. V nejjednodušší variantě jsou složeny z dvojice dílů. Permanentního magnetu a jazýčkového kontaktu z feromagnetického materiálu uloženého v nemagnetickém ochranném pouzdře. Působením magnetického pole magnetu dochází k sepnutí kontaktu a tím uzavření elektrického obvodu (viz obrázek 2.4a). Jeho rozpojení je posléze vyhodnoceno jako poplach.



(a) Princip magnetického kontaktu [36]


(b) Povrchová montáž [46]


(c) Skrytá montáž [46]

Obrázek 2.4: Magnetický kontakt. Princip a různé způsoby provedení.

Dle způsobu použití se vyrábí kontakty pro povrchovou montáž (obrázek 2.4b) nebo pro skrytou montáž (obrázek 2.4c). Výjimkou nejsou ani kontakty odolné nežádoucímu magnetickému poli. Ty obsahují více párů magnetů a jazýčkových kontaktů jak spínacích, tak rozpínacích. Působením rušivého vnějšího magnetického pole dojde vždy k rozpojení elektrického obvodu.

Magnetické kontakty jsou nejčastěji určeny pro zjišťování otevření oken nebo dveří. Chceme-li však vyhodnocovat rozbití skleněných ploch musíme zvolit jiný druh čidla. Jev při kterém se tříští sklo provází charakteristický zvuk a právě na něj čekají specializované senzory, aby vyhlásili poplach. V principu je získaný zvuk filtrován přes pásmové propusti a nadále vyhodnocován specifickou logikou. Kvalitnější čidla mají přirozeně sofistikovanější logiku vyhodnocující přítomnost tříštivého zvuku ve více částech zvukového spektra. Čímž lépe odolávají falešným poplachům.

2.3.3 Prvky prostorové ochrany

Ve vysoké míře se dnes používají ochranné prvky pro střežení prostorů, můžeme se také setkat s označením „čidla pohybu“. Není hlídáno přímo otevření vstupního otvoru, nýbrž přítomnost osoby na střeženém místě. V domácnostech se poslední dobou setkáváme s nahrazováním plášťové ochrany právě prvky prostorové ochrany. Z finančního hlediska je tento fakt pochopitelný. Naopak z bezpečnostního pohledu se připravujeme o taktickou výhodu. Reagujeme na narušitele, který už překonal mechanické zabezpečení a nachází se uvnitř naší domácnosti. Pachatel tak získává více času, čímž je o mnoho klidnější. Stejně jako ve většině podobných případů je vždy nejbezpečnější kombinace obou způsobů ochrany. V případě, že se rozhodujeme pro kompromis, musíme zvážit jeho výhody a nevýhody.

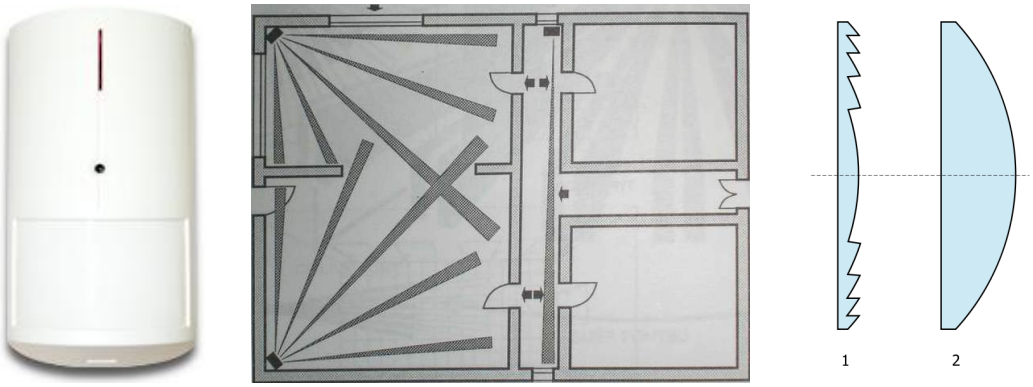
Čidla určená pro střežení prostor je možné rozdělit na dvě hlavní skupiny. První pouze registrují fyzikální změny ve svém pracovním prostředí, nazýváme je pasivní. Druhé aktivně působí na své okolí, a tak vytváří své vlastní fyzikální prostředí, ve kterém vyhodnocují

změny, nazýváme je aktivní. Pasivní čidla jsou dnes nejrozšířenější, a proto se seznámíme blíže s typickým zástupcem této skupiny, PIR čidlem (Passive infra red senzor, obrázek 2.5a) [44].

Pasivní čidlo pracující v infračerveném spektru elektromagnetického vlnění využívá skutečnosti, že každé těleso, jehož teplota je vyšší než -273°C a nižší než 560°C je zdrojem záření právě v tomto spektru. Teplota lidského těla poté odpovídá vlnové délce přibližně 9,4mm. Pyroelektrický senzor uvnitř čidla zachycuje pohyb těles mající různou teplotu od teploty okolí. Čidlo dále obsahuje propracovanou logiku, která posuzuje signály přijaté od senzoru a případně vyhlásí pohyb ve střeženém prostoru. Střežený prostor je oblast zorného pole čidla a závisí mimo jiné na použité optice.

Z finančních důvodů je častěji použita optika skládající se ze soustavy Fresnelových čoček [43]. Fresnelova čočka je vyráběna ze skla nebo plastu a její výhodu je mimo jiné nižší hmotnost, protože jsou z ní odstraněny ty části, které se přímo nepodílejí na lomu paprsků (obrázek 2.5c). Tím však vzniká obraz neodpovídající skutečnosti, což v těchto případech není kritické.

Protože pasivní čidla nevyzařují žádnou energii, je možné jich instalovat více a to i tak, aby se překrývala jejich zorná pole. Abychom předcházeli falešným poplachům od PIR čidel, musíme dodržet jisté zásady jejich instalace. Musí být nasměrovány tak, aby nereagovali na pohyb za okny nebo dveřmi. Nesmí být ozařovány přímými nebo nepřímými zdroji světla, zejména infračerveným. Také instalace PIR čidla poblíž ventilace, průvanu nebo podlahového vytápění není vhodná.



(a) PIR čidlo [44] (b) Správná instalace PIR čidel [36] (c) Fresnelova čočka 1 a klasická čočka 2 [43]

Obrázek 2.5: Správně instalovaná PIR čidla a v nich použita Fresnelova čočka.

2.3.4 Prvky tísňového hlášení

V případech, kdy je uživatel ohrožen na zdraví nebo životě jak svým, tak cizím přičiněním, je nesmírně důležité velmi rychle a jednoduše vyhlásit poplach. Prvky tísňového hlášení jsou především vybavena místa, kde hrozí přepadení za účelem zisku finančních prostředků. Typicky banky, čerpací stanice nebo pokladny v hypermarketech. V těchto případech se jedná o skryté prvky, které může obsluha nenápadně sepnout. Jedná se o vhodně tvarované mikrospínače umístěné například v podobě nožní spínací lišty na vnitřní straně desky stolu.

V prostorách mnohých veřejných budov jsou použity nouzové hlásiče požáru. Ty jsou instalovány takovým způsobem, aby je kdokoli mohl použít. Jsou na viditelných místech a patřičně označeny. Proti falešným nebo náhodným poplachům jsou chráněny skleněnou výplní, kterou je nutné pro použití hlásiče nejdříve rozbít.

V domácnostech se s takovým způsobem ochrany setkáváme velmi zřídka. Je to dáno především lhostejností a podceňováním těchto situací. Bohužel se v posledních letech setkáváme s nárůstem domácího násilí a loupežných přepadení osamocených seniorů. Nejen v těchto situacích je velice vhodné snadno, stisknutím jednoho tlačítka, přivolat pomoc.

Každý z nás má na tomto světě vyhrazený čas života, jehož délku naštěstí nikdo přesně nezná. Což ovšem znamená, že nás mohou zdravotní komplikace zasáhnout nečekaně v každé situaci. Přirozeně nejohroženější skupinou jsou lidé seniorského věku. Ačkoli mobilní telefon již podobným způsobem bezesporu zachránil spousty životů, tak se domnívám, že nouzové tlačítko by si v domácnostech vedlo stejně dobře a možná i lépe. V nejprostější variantě by akustickou signalizací dalo na vědomí sousedům. Přivolání pomoci by pak zajistili oni. Ideálně by se pomoc přivolala automaticky [39].

2.3.5 Pult centralizované ochrany

Pult centralizované ochrany (dále jen „PCO“) je místo, které je trvale obsluhované a do kterého se předávají informace o stavu jednoho nebo více EZS. Je možné se setkat i s pojmem poplachové přijímací centrum (dále jen „PPC“), které by mělo značit soukromou bezpečnostní agenturu. PCO pak označuje Policii. V praxi se však ustálil pouze pojem PCO bez rozlišení statutu provozovatele.

V případě potřeby, typicky při vyhlášení poplachu, vyšle bezpečnostní agentura na patřičné místo zásahové vozidlo. Členové této zásahové skupiny poté zjistí stav objektu, případně využijí služeb Policie nebo záchranných složek. Městská police Brno zřídila pro tento účel Jednotku operativního zásahu, která plní speciální úkoly při ohrožení života i zdraví a zabezpečuje výjezdy při porušení ochrany objektu napojeních na PCO [37].

Na tomto místě chci vyloučit celospolečenský názor, že PCO není určen pro běžné domácnosti a je velice finančně nákladný. Je sice pravdou, že PCO je ve vyšší míře využíván podnikatelskými subjekty, což ale nevylučuje možnost jeho použití v domácnosti. U vybraných bezpečnostních agentur začínají měsíční poplatky spojené s touto službou na několika stokorunách [22].

2.4 Elektrická požární signalizace

Ze statistiky Hasičského záchranného sboru ČR (dále jen „HZS“) pro rok 2009 plynou velice závažné údaje [13]. Na území celé České republiky vzniklo více než dvacet tisíc požárů, při kterých zahynulo 117 lidí a dalších 980 bylo s různou závažností zraněno. Pouze při požáru domácností, kterých vzniklo bezmála čtyři tisíce, bylo usmrceno přes 60 lidí. Což je více než polovina! Z těchto smutných dat bychom se měli poučit a snažit se snížit vytíženost HSZ, který musí denně řešit průměrně deset požárů domácností.

Od 1. července roku 2008 je v platnosti vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb, která zavádí povinnost použít zařízení pro autonomní detekci a signalizaci požáru ve všech novostavbách určených pro bydlení. V případě rodinných domů také zavádí povinnost vlastnit přenosný hasičský přístroj [12].

Následující text byl volně převzat z [36].

Mezi hlavní úkoly elektrické požární signalizace (dále jen „EPS“) patří okamžité a přesné určení místa vzniku požáru již v jeho samotném počátku, vyhlášení poplachu a řízení evakuačního systému. Ústředna požární signalizace vyhodnocuje stavy připojených čidel a v případě potřeby spustí poplach, případně přivolá pomoc. Od zabezpečovacího systému se požární signalizace odlišuje snad v jediné zásadní věci, která vychází z jejího účelu. Zabezpečovací systém ve většině případů pracuje ve dvou režimech. V nepřítomnosti uživatele pracuje v režimu „střežení“ a například otevření okna je okamžitě vyhlášeno jako poplach. Naopak v přítomnosti uživatele se EZS jeví jako vypnutý. EPS však pracuje neustále v režimu „střežení“. V přítomnosti uživatele tak nechrání pouze jeho majetek, nýbrž i jeho život a zdraví. Protože tyto dva bezpečnostní systémy si jsou velice podobné, nabízí se myšlenka jejich vzájemné kombinace.

EZS pokud nabízí možnost pracovat i jako EPS musí být schopen ve všech režimech jeho činnosti vždy vyhodnocovat stavy požárních čidel. Nikdy nesmí nastat stav, kdy jsou tato čidla odpojena a nehlídána. Ovšem pokud si tak uživatel výslovně nepřeje, například vlivem technické poruchy. Schopnosti reagovat na bezpečnostní hrozbu jsou pak dány připojenými čidly. S těmi základními se v následujícím textu v krátkosti seznámíme.

2.4.1 Hlásiče teplotní

Pokud by se laik zamýšlel nad způsobem detekce vznikajícího požáru, nejspíše by mu neunikl fakt, že při tomto jevu dochází k náhlému zvýšení teploty. A právě teplotní hlásiče sledují tuto veličinu. V jednodušším případě porovnávají aktuální naměřenou teplotu s trvale nastavenou prahovou teplotou. Při jejím překročení čidlo hlásí ústředně vznikající požár. V jednoduchosti je síla, avšak ta s sebou přináší jisté nevýhody. Tou hlavní je právě nastavení prahové teploty. Pokud bude příliš nízká, bude systém náchylný na falešné poplachy. Naopak pokud bude příliš vysoká, bude systém reagovat později, požár napáchá vyšší škody a v krajním případě nebude možnost jej svépomocí uhasit.

Ovšem nemusíme porovnávat absolutní hodnotu naměřené teploty, nýbrž rychlost jejího zvýšení. Teplota je měřena jak uvnitř čidla, tak i na jeho povrchu. Vlivem tepelné setrvačnosti je při požáru nejdříve vyhodnocena teplota okolí, čímž dochází k rozdílu teploty mezi senzory na povrchu a uvnitř čidla. Pokud tento rozdíl překročí jistou hodnotu, je ústředně předán signál poplachu. Opět i zde platí, že kombinace obou principů přináší nejspolehlivější výsledky. Obrázek 2.6a ukazuje průběh změny teploty při začínajícím požáru.

2.4.2 Optické hlásiče kouře

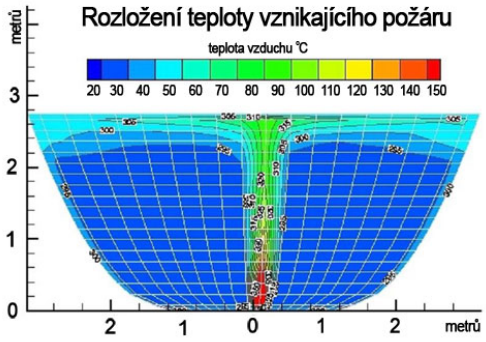
Další vlastností požáru, které si laik jistě povšimne je všudypřítomný kouř. Hasič by mohl vyprávět, jak právě kouř snižuje viditelnost a činní tak jeho zásah obtížnější. Co je však nepřítelem hasičů, tak může na druhé straně sloužit pro odhalení začínajícího požáru. Čidla jsou pro optickou detekci kouře vybavena zdrojem světla a světlocitlivým prvkem. Typicky LED diodou (Light-emitting diode) a fotodiodou. Oba tyto prvky jsou v uzavřené trubici, do které může proniknout pouze kouř, nikoli cizí zdroj světla. Od kouře se odrazí světelný paprsek produkovaný LED diodou a dopadne na fotodiodu. Elektronika čidla tuto událost zaregistruje a ústřednu informuje o poplachu.

Optické hlásiče kouře patří v dnešní době mezi nejpoužívanější. Jsou spolehlivé a nejsou příliš náchylné k planým poplachům. Kritické pro ně je tvorba orosení a různé druhy výparů. Správné umístění optického hlásiče ukazuje obrázek 2.6b a dále na obrázku 2.6c je jedno z typických provedení takového hlásiče.

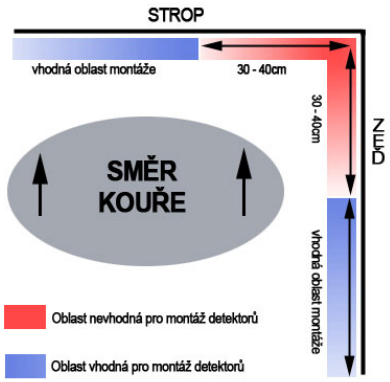
2.4.3 Tlakové hlásiče

V předchozích případech jsou neznalému doprovázející okolnosti požárů dobře známé, avšak princip tlakových hlásičů už tak dobře znám není. Tlakové hlásiče se skládají z vyhodnocovací jednotky a snímací trubice. Kompresor uvnitř vyhodnocovací jednotky v pravidelných intervalech vytváří přesně definovaný přetlak ve snímací trubici. Pokud dojde ke zvýšení okolní teploty, změní se tlak vzduchu ve snímací trubici a vyhodnocovací jednotka informuje ústřednu o poplachu.

Výhodou těchto hlásičů je možnost instalovat snímací trubici na libovolné místo. Neovlivňují ji téměř žádné okolní faktory, tedy ani vlhkost, ani prach a ani hmyz. Používají se nejčastěji pro ochranu konkrétních zařízení nebo tam, kde není možné použít jiný druh hlásiče.



(a) Rozložení teploty vznikajícího požáru [48]



(b) Správná instalace hlásiče kouře [48]

(c) Optický hlásič kouře [15]

Obrázek 2.6: Optický hlásič kouře, jeho správná instalace a vývoj teploty při vzniku požáru.

Kapitola 3

Použitá bezdrátová komunikace

Moderní společnost je mimo jiné poznamenaná chtíčem mít vše snadno a pohodlně dostupné. Všudypřítomné kabely tuto touhu výrazně omezují, a tak vznikají různé technologie nahrazující kabelová spojení. Snad jen velmi otrlý jedinec si dnes dovede představit používat pevně připojený ovladač k televizi. Prostředky pro použití bezdrátové komunikace již nejsou pouze doménou profesionálních zařízení. Jsou již cenově natolik dostupné, že se přímo nabízí jejich použití ve vlastních projektech.

Bezdrátovou komunikaci můžeme rozlišovat podle několika kritérií. Rádiové moduly pracující v různých kmitočtových pásmech, používající různé protokoly komunikace. Optické moduly komunikující na přímou viditelnost pracující s laserovým paprskem nebo světlem například v infračerveném spektru. Můžeme ji však také rozlišit dle směru komunikace na jednosměrný a obousměrný.

Jednosměrná komunikace se vyznačuje vysílacím prvkem na straně jedné a na straně druhé prvkem přijímacím. Vysílač pošle určitou informaci, která je v ideálním případě v pořádku doručena. Protože přijímací prvek není vybaven vysílačem, tak odesílatel nemůže obdržet zpětnou vazbu o stavu doručení nebo nedoručení jím vyslané zprávy. V zabezpečovací technice to s sebou přináší jistá úskalí.

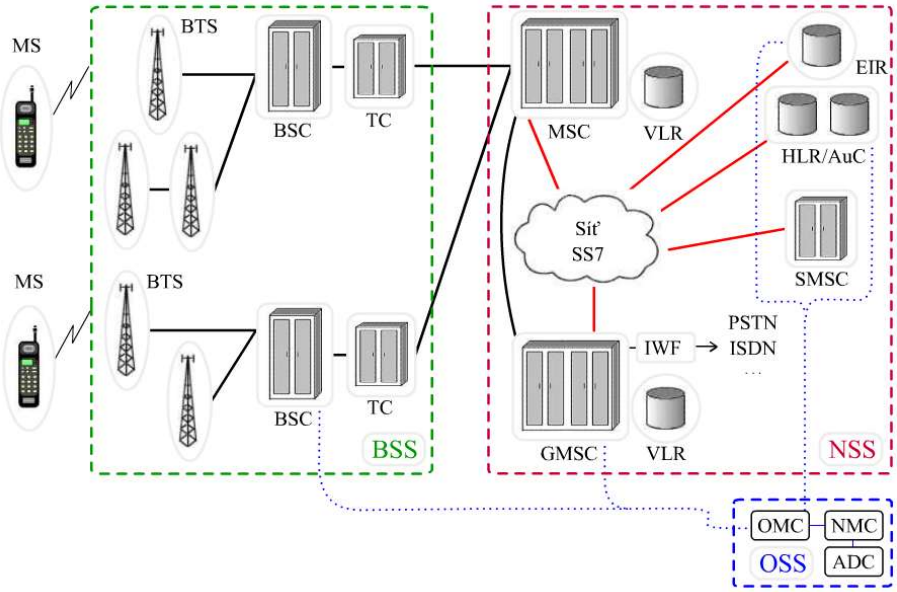
Ústředna je typicky vybavena přijímacím prvkem a senzory vysílači. Aby mohli být senzory bezdrátové, jsou napájeny z vlastních baterií. Baterie mají omezenou kapacitu, čímž je kladen na čidla důraz nízké spotřeby energie. S každou vyslanou zprávou se tak určitá část energie spotřebuje. Problém nastává v případě, kdy je systém neaktivní. Bezdrátové čidlo zaznamená pohyb, vyšle zprávu ústředně a ta ji ignoruje. V případech zvýšeného pohybu v prostoru čidla, tak můžeme velmi rychle vybít jeho baterii [36].

Zmíněné nedostatky řeší oboustranná komunikace. Každý prvek je vybaven vysílačem a přijímačem. Takový prvek označujeme jako transceiver. Pojem transceiver vznikl spojením anglických slov označující právě vysílač a přijímač, tedy transmitter a receiver. Jednotlivé moduly vybavené transceiverem si tak mohou předávat zprávy o stavu doručení, udržovat konektivitu apod. V zabezpečovací technice má tento způsob komunikace snad samé výhody. Při zapnutí si ústředna zkontroluje funkčnost všech připojených čidel, které bude posléze informovat o přechodu do stavu „nestřeženo“. Čidla v tomto stavu nebudou vysílat žádné zprávy a budou šetřit své baterie. V případě, kdy čidlo informuje ústřednu o poplachu, si ústředna může tuto skutečnost nechat od čidla znovu ověřit. Sníží se tím riziko vyvolání planého poplachu [36].

V následujícím textu se seznámíme s bezdrátovými technologiemi, které jsem použil při návrhu zabezpečovacího zařízení.

3.1 Technologie GSM

Pokud řekneme bezdrátová komunikace, většině lidí se vybaví mobilní telefon. Technologie GSM (Global System for Mobile Communication, původně Groupe Spécial Mobile) byla prohlášena standardem v roce 1990 a dnes ji využívá přes tři miliardy uživatelů. O prudkém rozvoji této technologie také vypovídá skutečnost, že první SMS zpráva (Short Message Service) byla poslána v roce 1992 a o třináct let později jejich roční počet překročil hranici jednoho bilionu [10].



Obrázek 3.1: Blokové schéma technologie GSM [30]

Síť GSM tvoří čtyři hlavní bloky, obrázek 3.1. Koncovým zařízením je mobilní uživatelská stanice („MS“ - mobile station). Ta obsahuje mobilní zařízení („ME“ - mobile equipment) skládající se z transceiveru, mikrofonu, reproduktoru, klávesnice, displeje a patřičné elektroniky. Mobilní zařízení je jednoznačně identifikovatelné číslem IMEI (International Mobile Equipment Identity), které je uložené v jeho paměti. Nezbytnou součástí MS je karta SIM (Subscriber Identification Module), bez které je možné uskutečnit pouze tísňové volání na číslo 112. Karta SIM zajišťuje ověření a identifikaci uživatele, včetně služeb jemu přístupných [30].

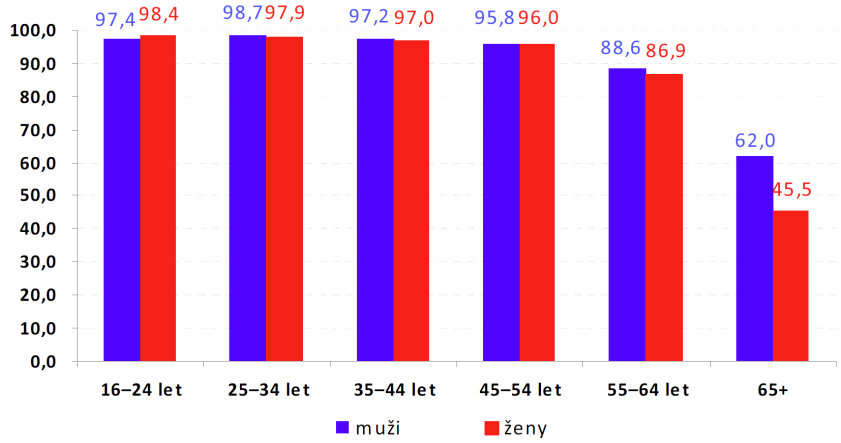
MS prostřednictvím rádiového spojení komunikují se základnovou stanicí („BTS“ - base transceiver station), která je členem subsystému základnových stanic („BSS“ - base station subsystem). Skupina BTS je pak společně řízena základnovou řídící jednotkou („BCS“ - base station controller) a mohou tak vytvářet libovolnou síťovou topologii. Mobilní ústředna („MCS“ - mobile switching center) patří do síťového spojovacího subsystému („NSS“ - network switching subsystem) a mimo obvyklých přepojovacích funkcí vykonává činnosti spojené s mobilitou účastníků, například určování jejich polohy. MCS slouží také jako brána do okolních telekomunikačních sítí jak mobilních, tak i pevných [30].

Velmi důležitou součástí každé GSM sítě je domovský lokační registr („HLR“ - home location register). V něm jsou uložena všechna důležitá data o účastnicích dané sítě, například jejich poloha. Na tento registr je napojena databáze mobilních stanic („EIR“ - equipment

identity register) obsahující čísla IMEI mobilních stanic, které jsou autorizovány k použití v dané síti nebo jsou nahlášena jako odcizená [30].

3.1.1 Využití GSM v zabezpečovací technice

Dle zprávy Českého statistického úřadu v roce 2008 vlastní mobilní telefon přes 95% obyvatel České republiky [47], což potvrzuje graf 3.2. V nutných případech záchranné složky vyhledávají osobu v nouzi pomocí jejího mobilního telefonu. Vycházejí přitom ze skutečnosti, že většina majitelů mobilního telefonu nosí tento přístroj neustále při sobě. S výhodou toho však můžeme využít i v zabezpečovací technice.



Obrázek 3.2: Muži a ženy využívající mobilní telefon, v procentech [47]

Informovat o aktuálním stavu domácnosti za použití mobilního telefonu můžeme v zásadě trojím způsobem. Běžným hovorem můžeme přehrát předem nahranou zprávu nebo pouze prozvoněním informovat o určité události v domácnosti. SMS zprávou v určitém textovém formátu sdělíme konkrétní událost. Většina mobilních telefonů je schopna odeslat i přijmout MMS zprávu (Multimedia Messaging Service), do které můžeme vložit nejenom text, ale i fotografie, video, případně zvukový záznam. Rušit signál mobilního telefonu je technicky náročné a proto lze považovat tento způsob komunikace za spolehlivý.

Každý uživatel EZS je jednoznačně identifikován pomocí vlastního telefonního čísla. V případě potřeby se můžeme rozhodnout, kterého uživatele budeme informovat. Můžeme předat zprávu uživateli, který se systémem pracoval jako poslední. Nebo zasláním SMS zprávy na každé telefonní číslo, informujeme všechny uživatele současně. Kterého uživatele a v jakém pořadí je budeme informovat, se můžeme rozhodnou na základě předem nastavených priorit. Stav poplachu, tak budeme raději hlásit nejdříve na mobilní telefon hlavy rodiny a posléze případně dalším členům domácnosti.

Jistou výhodou při použití GSM technologie v zabezpečovacím systému je také přenos poplachu na PCO. V reálném čase se bezpečnostní agentura dozvídá o potřebě zasáhnout v naší domácnosti a bez delších časových prodlev vysílá na místo zásahové vozidlo.

Uživatelé však nemusí od EZS pouze přijímat zprávy, ale v případě potřeby mohou systém vzdáleně ovlivňovat. V tomto případě způsob vzdáleného ovládání závisí na konkrétní implementaci systému. Nejčastěji se však provádí zasláním SMS zprávy v definovaném formátu. Identifikace uživatele se provede pomocí telefonního čísla odesílatele a autentizace se typicky provádí vložením hesla do obsahu zprávy. Je možné se setkat i se způsobem, kdy

EZS přijme požadavek a vygeneruje určitý kód, který zašle zpět na telefonní číslo uživatele. Přijatý požadavek však EZS vykoná až poté, co uživatel zašle zpět vygenerovaný kód. Tato metoda zabraňuje podvržení telefonního čísla odesílatele za telefonní číslo uživatele.

3.1.2 Vlastnosti dostupných GSM modulů

Pro komunikace vestavěného systému s mobilním telefonem je nutné použít speciální rozhraní, konkrétně GSM modem. V následujícím textu se seznámíme s vlastnostmi dvou GSM modulů, které jsou běžně dostupné na našem trhu.

Telit GC864-QUAD

GSM modul Telit GC864 (obrázek 3.3a) je velmi malý a lehký, vyniká nízkou spotřebou a je schopen pracovat ve všech GSM sítích současnosti. Konkrétně na kmitočtech 850, 900, 1800 a 1900MHz. Připojuje se do vestavěného systému pomocí 80ti pinového konektoru Molex, umístěného na jeho spodní straně. Na jeho horní straně je místo pro pouzdro SIM karty. Pro připojení GSM antény nabízí 50Ω Murata konektor MXTK92. Modul je vyhovující požadavkům EU (Evropská unie) RoHS (Restriction of Hazardous Substances. Zákaz použití nebezpečných látek) (EU direktiva 2002/95EG). Bližší informace o modulu lze nalézt [40].

Přehled vlastností GSM modulu:

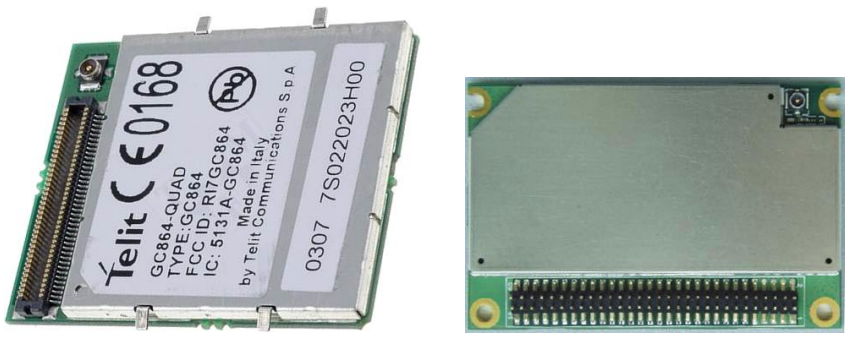
- Rozměry 36,2mm x 30mm x 3,2mm, hmotnost 6,1g
- Provozní teplota -40°C – +85°C.
- Výstupní výkon - Class 4 (2W) @ 850/900MHz, Class 1 (1W) @ 1800/1900MHz.
- Antenní Murata konektor MXTK92 / 50Ω.
- Napájení 3,22V – 4,5V DC, proudový odběr při hovoru 200mA, 370mA při datovém přenosu GPRS. Špičkový, krátkodobý odběr až 2A.
- Připojení přes 80ti pinový konektor Molex.
- Podpora SIM karet pracující při napětí 1,8V nebo 3V. Je vybaven pouzdrem na SIM kartu.
- Komunikace s mikrokontrolérem přes rozhraní UART (Universal Asynchronous Receive Transmit).
- 21 I/O pinů, 3 x A/D převodník, 1 x D/A převodník, 2 mikrofonní vstupy a 2 reproduktorové výstupy.
- Vestavěný TCP/IP stack.
- RoHS vyhovující
- Cena 2 800Kč [41].

SIMCom SIM300C

GSM modul SIM300C od firmy SIMCom (obrázek 3.3b) je schopen pracovat v GSM sítích na kmitočtu 900, 1800 a 1900MHz. K vestavěnému systému se připojí pomocí 60ti pinového DIP konektoru s roztečí 1,27mm. Na rozdíl od předchozího modulu není možné k němu přímo připojit SIM kartu, pro kterou má vyhrazeny pouze piny na zmíněném konektoru. Vyhovuje požadavku RoHS. Velice patrný rozdíl mezi těmito moduly panuje v jejich pořizovací ceně. Modul SIM300C je pět krát levnější než modul od firmy Telit. Bližší informace o modulu lze nalézt [32].

Přehled vlastností GSM modulu:

- Rozměry 50mm x 36mm x 6,2mm, hmotnost 13,8g
- Provozní teplota -40°C – +85°C.
- Výstupní výkon - Class 4 (2W) @ 900MHz, Class 1 (1W) @ 1800/1900MHz.
- Antenní Murata konektor MXTK92 / 50Ω.
- Napájení 3,4V – 4,5V DC, proudový odběr při hovoru 260mA, 470mA při datovém přenosu GPRS. Špičkový, krátkodobý odběr až 3A.
- Připojení přes 60ti pinový DIP konektor.
- Podpora SIM karet pracující při napětí 1,8V nebo 3V.
- Komunikace s mikrokontrolérem přes rozhraní UART.
- 3 I/O piny, 1 x A/D převodník, 2 mikrofonní vstupy a 2 reproduktorové výstupy.
- Vestavěný TCP/IP stack.
- RoHS vyhovující
- Cena 555Kč [41].



(a) Telit GC864-QUAD [40] (b) SIMCom SIM300C [32]

Obrázek 3.3: Běžně dostupné GSM moduly

3.2 Technologie ZigBee IEEE 802.15.4

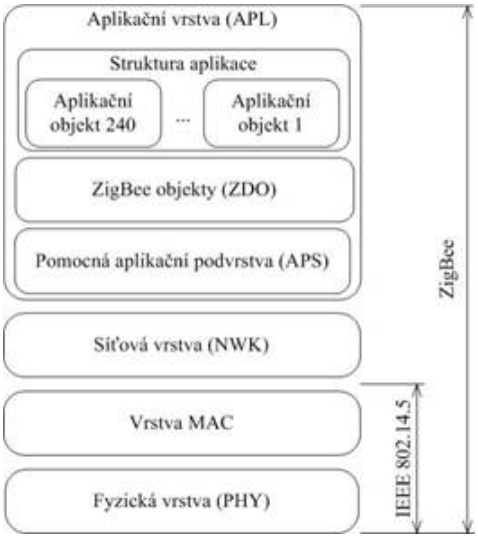
ZigBee je oficiálně bezdrátový síťový protokol navržený pro použití v senzorových sítích s nízkým požadavkem na datovou přenosovou rychlost a velmi nízkou spotřebou energie. Standard IEEE (The Institute of Electrical and Electronics Engineers) 802.15.4 byl dokončen v roce 2003 a zajišťuje základní funkčnost protokolu ZigBee. Protokol ZigBee je v tomto ohledu podobný protokolu TCP/IP, který také využívá služeb standardu IEEE 802.11b nebo 802.3 [6].

3.2.1 Referenční síťový model

Referenční síťový model protokolu ZigBee (obrázek 3.4) vychází ze sedmivrstvého modelu ISO/OSI, podrobněji v kapitole 4.1.2. Standard IEEE 802.15.4 definuje dvě nejnižší vrstvy modelu. Fyzická vrstva PHY je odpovědná za samotnou bezdrátovou komunikaci. Pracuje ve třech bezlicenčních rádiových pásem ISM (Industrial, Scientific, Medical) s celkovým počtem 27 využitelných kanálů. Jednotlivá rádiová pásma a jejich vlastnosti jsou obsahem tabulky 3.1.

Vrstva MAC zajišťuje spojení a odpojení se sítí, zabezpečení komunikace, řízení toku (flow control), potvrzení přijatých dat, znovu odeslání ztracených dat a vyšším vrstvám protokolu ZigBee nabízí své rozhraní. V jednom paketu je možné odeslat nejvýše 127B vlastních dat. Pro snížení chybovosti jsou tato data vybavena 16b kontrolním součtem CRC.

Aplikační vrstva je složena z pomocné aplikační podvrstvy (APS - application support sub-layer), z objektů ZigBee (ZDO - ZigBee device object) a z aplikačních objektů definovaných výrobci. Úkolem pomocné aplikační podvrstvy je umožnit propojit dvě zařízení na základě jejich služeb a potřeb. Dále přeposílá zprávy mezi vzájemně vázanými zařízeními. Objekt ZigBee (ZDO) definuje roli zařízení v síti a zajišťuje hledání dalších zařízení v síti, od kterých zjišťuje jimi poskytované služby [17].



Obrázek 3.4: Referenční síťový model protokolu ZigBee [17]

ISM pásmo [MHz]	Počet kanálů	Číslo kanálu	Přenosová rychlost [kbps]
868	1	0	20
915	10	1 — 10	40
2400	16	11 — 26	250

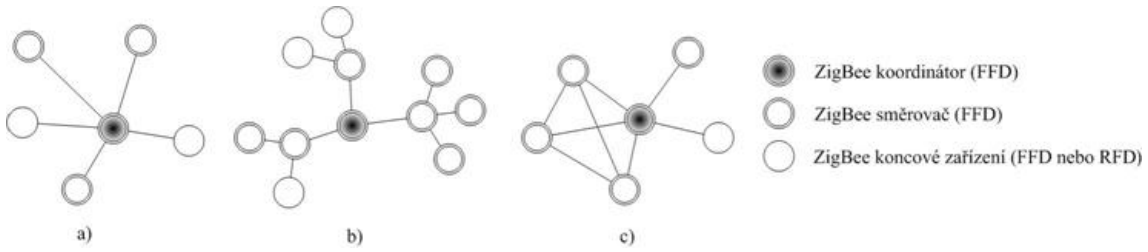
Tabulka 3.1: Používaná bezlicenční rádiová pásma protokolem ZigBee

3.2.2 Topologie sítě

Standard IEEE 802.15.4 rozeznává dva druhy zařízení. Plně funkční zařízení (FFD - full function device) a redukovaná zařízení (RFD - reduce function device). FFD jsou typicky napájeny z neomezeného zdroje elektrické energie a jsou většinu svého času připojeny do sítě. Na druhou stranu RFD jsou napájeny z vlastních baterií a mají za úkol jednou za čas odeslat určité informace dalšímu zařízení. Většinu svého času pracují v režimu spánku.

Protokol ZigBee přebírá předchozí koncept a definuje tři zařízení s obdobnými funkcemi. ZigBee koordinátor sítě je druh FFD a zajišťuje funkčnost sítě. Vytváří síť, alokuje adresy pro zařízení, které mají povolené se připojit do sítě a vytváří komunikační most mezi RFD klienty. Dalším zařízením je koncový klient. Může se ve skutečnosti jednat jak o FFD, tak i o RFD, což závisí na účelu tohoto zařízení. Posledním definovaným zařízením je směrovač (router). Jeho úkolem je zvýšit fyzický dosah sítě. Protože se jedná o FFD zařízení, tak může směrovač vykonávat i funkci koncového klienta [6].

Síťová vrstva protokolu ZigBee podporuje topologie typu hvězda (star), síť (mesh) a strom (tree), viz obrázek 3.5. V topologii typu hvězda komunikují koncoví klienti přímo s koordinátorem sítě. Topologie typu síť umožňuje komunikace mezi dvěma rovnocennými klienty, spojení peer-to-peer.



Obrázek 3.5: Topologie sítě protokolu ZigBee [17]

3.2.3 Použití v zabezpečovací technice

Tak jako ve spoustě jiných odvětví, se i v zabezpečovací technice stále více uplatňuje bezdrátová komunikace mezi jednotlivými prvky zařízení. Naprostá většina lidí si zabezpečení pořizuje až do zařízené domácnosti. Možnost vyhnout se použití kabelových vodičů v tomto případě velice ocení. V nejjednodušší variantě je nutné zapojit ústřednu do zásuvky a rozmístit čidla prostorové ochrany, které jsou napájené z vlastních baterií. Takový úkol zvládne i naprostý laik.

Také případné změny v systému jsou snadné. Připojit nové čidlo nebo nahradit to současné je otázkou několika minut. V českých domácnostech, které rozhodně nebudou

světovou výjimkou, se docela často přemísťuje nábytek. Po chvíli současné rozložení nábytku zevšední a jeho přemístěním získá domácnost nový nádech. Když používáme bezdrátová čidla a zjistíme, že jsme si jedno z nich zastínili posunutou skříní, není nic jednoduššího než čidlo přenést někam, kde mu v jeho funkci nic nebrání. S klasickým drátovým systémem bychom museli natahovat novou kabeláž, případně přivolat odborného technika.

Jakmile jednou investujeme mnohdy nemalé finanční prostředky do bezdrátového EZS, nemusí nutně stěhování do nové domácnosti znamenat nákup nového EZS. Stejně jak je snadná montáž, tak je snadná demontáž. Lidé, kteří nevlastní svoji nemovitost a žijí v pronajaté domácnosti, si mohou konečně dopřát pocit bezpečí bez ohledu na majitele nemovitosti. S trochou nadsázky, lze říci, že takový systém je možné si vzít s sebou i na dovolenou.

3.2.4 Popis vlastností modulu X-Bee

Pro komunikaci nad standardem IEEE 802.15.4 jsem zvolil výrobek od firmy Digi International (dříve MaxStream). Konkrétně se jedná o modul XBee, obrázek 3.6. Tento modul pracuje v bezlicenčním rádiovém pásmu 2,4GHz s přenosovou rychlostí až 250kbps. Svými rozměry není o mnoho větší než dvacetikoruna, což ve spojení s velmi nízkou spotřebou energie činní tento modul velice vhodný pro použití v zabezpečovací technice. Nabízí dva režimy práce. V transparentním režimu všechna data přijatá přes rozhraní UART posílá bezdrátově svému protějšku, který je pošle na výstup přes své rozhraní UART. Jak příjemce, tak odesílatel nemusí mít ani tušení, že mezi sebou komunikují bezdrátově. Druhý režim je alternativou k transparentnímu módu a nabízí vlastní API (Application programming interface) rozhraní pro řízení bezdrátové komunikace. Bližší informace o modulu v katalogovém listu výrobce [4].

Obrázek 3.6: XBee modul, měřítko 1:1

Přehled vybraných vlastností XBee modulu:

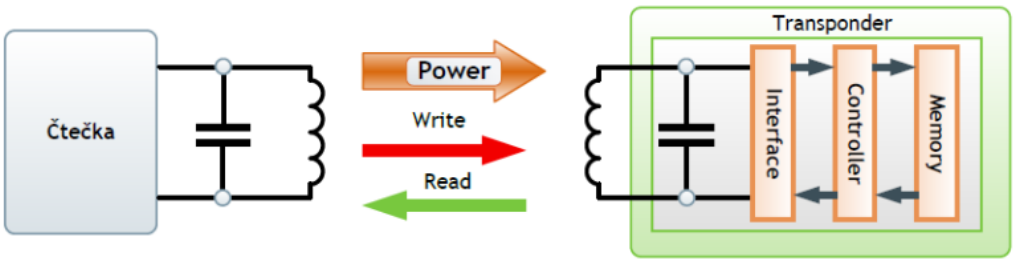
- Rozměry 24mm x 27mm x 2mm
- Provozní teplota -40°C – +85°C.
- Výstupní výkon 1mW, v budově dosah až 30m
- Integrovaná keramická anténa nebo konektor SMA pro připojení externí antény
- Napájení 2,8V – 3,4V DC, proudový odběr při vysílání 45mA a 55mA při příjmu dat. Klidový odběr menší než 10μA.
- Komunikace s mikrokontrolérem přes rozhraní UART.
- Až 8 x I/O piny nebo 8 x A/D převodník, 2 x PWM (puls width modulation)
- Velmi jednoduchá a rychlá použitelnost v transparentním režimu

3.3 Technologie RFID

Ačkoli bychom si to vždy uvědomili, používáme radiofrekvenční identifikaci (RFID - radio frequency identification) pokaždé, když nastartujeme automobil. Většina moderních aut je vybavena imobilizérem, který odpojuje přívod paliva do motoru. Klíč používaný k nastartování obsahuje jednoznačně identifikovatelný čip, který imobilizér zná. Pokud použijeme jiný klíč, nebude možné nastartovat.

Systém RFID se skládá ze tří komponent. Z transpondéru (někdy označován jako tag), z čtečky a z řídících prvků. Transpondér obsahuje identifikační číslo, které může být za jistých okolností světově jedinečné. Případně je vybaven dodatečnou pamětí pro uložení vlastních dat [27].

Z hlediska napájení rozlišujeme transpondéry na aktivní, semiaktivní a pasivní. Aktivní jsou vybaveny baterií a vysílají do okolí signál, který zachycují čtečky. Pasivní žádnou baterii nemají, a tedy nemohou samy nic vysílat. K tomuto účelů využívají elektromagnetické pole čtečky, které v transpondéru indukuje napětí. Usměrněný elektrický proud pak nabíjí kondenzátor a po jeho nabití napájí řídící obvod transpondéru, který zahájí odesílání dat (viz obrázek 3.7). Semiaktivní transpondéry jsou vybaveny baterií, ale ta slouží pouze k zesílení signálu, a tedy ke zvýšení jeho dosahu.



Obrázek 3.7: Princip technologie RFID [20]

Čtečky jsou zařízení, které mají za úkol zachytit vysílání dat z transpondéru, zpracovat je a předat v definované podobě řídícím zařízením. Mohou však být také schopné zápisu dat do přídavné paměti transpondéru. Pro vysílání i příjem dat používá čtečka anténu, která může být umístěna v pouzdře čtečky nebo externě. Pro správnou funkci musí RFID čtečka a transpondér pracovat na stejné frekvenci [20].

3.3.1 Použití RFID v zabezpečovací technice

Na začátku podkapitoly o RFID jsem zmínil použití této technologie v zabezpečení automobilů. Podobné využití je možné praktikovat i při zabezpečení domácností. Transpondéry jsou vyráběny mnoha velikostech a provedeních. Často se setkáme s provedením v podobě malé kartičky nebo přívěšku na klíče, viz obrázek 3.8. Karta se svými rozměry pohodlně vleze do peněženky, přívěšek na klíče také uživatele neobtěžuje.

Technologie RFID postupně vytlačuje ve větších firemních budovách mechanické klíče. Ve spojení s elektronickými zámky se vytváří možnost snadného přidělování oprávnění přístupu. Ředitel firmy může mít díky jediné kartě přístup kdekoli, kdežto jeho podřízený pouze ke svému pracovišti. Ztráta nebo případné odcizení karty není pro firmu taková

pohroma, jako ztráta klíče. Nemusí přenastavovat zámky a zaměstnance vybavovat novými klíči. Stačí pouze ztracenou kartu zablokovat a do systému přidat kartu zcela novou.

Pro domácnost není až tak finančně kritická situace ztráty klíče. Členů rodiny nebývá z pravidla tolik, aby to byl fakt, který přesvědčí k použití RFID. Tím by měla být právě možnost okamžité reakce na ztrátu transpondéru. S použitím systému komunikujícím přes mobilní telefon, tak pomocí jediné SMS zprávy zablokujeme ztracenou kartu. Případný zloděj, tak nebude schopen vstoupit do domácnosti nebo odblokovat EZS. Pokud není systém vybaven GSM komunikací, tak je alespoň snadnější kartu zablokovat přes počítač než vyměnit celý zámek společně s ostatními klíči.

(a) Přívěšek na klíče [34] (b) Karta, rozměry 54mm x 85mm [34] (c) Čtečka ID12 [14]

Obrázek 3.8: Vybrané druhy transpondérů a jejich čtečka

3.3.2 Vlastnosti RFID čtečky ID12

Abych mohl ve své práci využít technologii RFID, musel jsem zvolit vhodnou čtečku. Tou se ukázal být modul ID12 od firmy ID Innovations [14], viz obrázek 3.8c. Ve svém skutečně malém pouzdře ukrývá interní anténu, což usnadňuje celkový návrh aplikace. Čtečka pracuje na kmitočtu 125kHz a zvládá pouze čtení z karet ve formátu EM4001 a jemu kompatibilním s kódováním Manchester 64b. Výrobce uvádí čtecí vzdálenost 120mm a více. Řídícímu mikrokontroléru předává data pomocí protokolu Wiegand26 (viz [11] nebo ve formátu ASCII (American Standard Code for Information Interchange) přes rozhraní UART.

Přehled vybraných vlastností RFID modulu ID12:

- Rozměry 25mm x 26mm x 6mm.
- Pracovní kmitočet 125kHz, kompatibilní s formátem EM4001 s kódováním Manchester 64b.
- Integrovaná anténa nebo možnost připojení externí antény pro zvýšení čtecího dosahu.
- Napájení 4,6V – 5,4V DC, proudový odběr 30mA.
- Komunikace s mikrokontrolérem přes rozhraní UART ve formátu ASCII nebo protokolem Wiegang26.

Kapitola 4

Použité technologie pro komunikaci s počítačem

Komfortu nabízeného uživateli není nikdy dostatek. Často je potřeba něco přidat, něco ubrat nebo změnit. Pokud uživatel není schopen změnu svépomocí zvládnout, bývá zvykem přivolávat odborného technika. Pro každého, kdo bude chtít systém přizpůsobit bude snazší použít například přenosný počítat než specializované zařízení. Absolutní většina přenosných počítačů je dnes vybavena konektorem RJ45 pro připojení do sítě Ethernet a konektorem pro připojení zařízení přes rozhraní USB. Těmto dvěma technologiím se budu věnovat v následujícím textu.

4.1 Technologie Ethernet a sítě TCP/IP

Dnešní moderní společnost lze charakterizovat jedním slovem: „Internet“. Rozvoj tohoto média v posledních letech nabyl obrovských rozměrů a s tím souvisí i dostupnost komponent umožňující jeho využití. Čím více se internet zabydluje v běžných činnostech, jako je například nakupování, tím více roste touha mít internet i tam, kde se zatím nepoužívá.

Způsobů, kterými lze připojit vestavěný systém do sítě internet je více. Protože se tato práce věnuje návrhu a konstrukci EZS, tak budu předpokládat jeho připojení do místní sítě LAN (local area network). Ta dle možností uživatele pak může být součástí rozlehlé sítě WAN (wide area network), tedy i internetu. K připojení do sítě LAN jsem zvolil dnes nejrozšířenější rozhraní Ethernet.

4.1.1 Popis rozhraní Ethernet

Tato podkapitola byla volně převzata z [2].

Protokol Ethernet byl normalizován standardem IEEE 802.3 v roce 1985. Vychází z původního návrhu protokolu DIX Ethernet, jehož název plyne z prvních písmen firem DEC, Intel a Xerox, které ho vytvořili o pět let dříve.

Standard IEEE 802.3 popisuje elektrické vlastnosti transceiverů, mechanické vlastnosti konektorů a kabelů a způsoby jakými jednotlivé prvky sítě jsou identifikovatelné a jak mezi sebou sdílí komunikační médium. Protože se standard neustále vyvíjí, tak dnes obsahuje velkou řadu rozšiřujících pravidel. Například můžeme rozlišit Ethernet dle rychlosti síťové komunikace. Originální standard pracoval s rychlostí 10Mb/s, dnes nejčastěji používaný

Ethernet komunikuje rychlostí 100Mb/s a je znám pod názvem Fast Ethernet. Výjimkou není ani rychlost 1Gb/s (Gigabit Ethernet) nebo 10Gb/s.

Všechna data v Ethernetové síti jsou přenášena ve strukturách nazývaných rámce (anglicky frames). Tento rámec obsahuje pole pro data a další informace umožňující jej doručit na správné místo v síti, viz tabulka 4.1.

Název pole	**Délka v bytech**	**Účel**
Synchronizace	8	Ethernet je asynchronní rozhraní, proto potřebuje synchronizaci, aby příjemce mohl bezchybně přijmout další data.
Adresa cíle	6	Hardwarová adresa, známá také jako MAC adresa (Media Access Control address). Prvních 24b určuje výrobce zařízení, dalších 24b identifikuje zařízení samotné.
Adresa zdroje	6	MAC adresa odesílatele.
Délka / druh	2	Je-li hodnota nižší než 1500, tak určuje délku dat v bytech. Je-li vyšší než 1536, tak určuje protokol, který používá obsah dat.
Data	46–1500	Samotná data, které posílá odesílatel příjemci. Méně než 46B dat není možné odeslat. V případě potřeby jsou doplněny daty bez významu. Vyšší množství dat je rozděleno do více rámců.
Kontrolní součet	4	Odesílatel z posílaných dat vytvoří kontrolní CRC (cyclic redundacy check) součet, který musí souhlasit se součtem vytvořeným příjemcem. Pokud obě hodnoty nesouhlasí, došlo při přenosu k chybě.

Tabulka 4.1: Ethernetový rámec dle standardu IEEE 802.3

4.1.2 Síťový model ISO/OSI

V roce 1984 organizace ISO (International organization for standardization) vypracovala referenční model ISO/OSI (International organization for standardization / Open system interconnection). Do té doby každý větší výrobce používal svůj vlastní model, což stavělo do nevýhodné pozice menší subjekty. Pokus o vytvoření otevřeného modelu se však nepodařilo uplatnit v masové míře, zejména kvůli pomalému standardizačnímu procesu.

Model ISO/OSI rozděluje síťovou komunikaci do sedmi vrstev, kde každá vrstva plní určitou funkci a poskytuje své prostředky vrstvě vyšší. Při postupném předávání odesílaných dat do nižších vrstev, se data zapouzdřují do jejich struktur, až jsou nakonec odeslána přes komunikační médium. Protějšek přijatá data postupně rozbaluje a nakonec jsou předána vrstvě nejvyšší, kde jsou zpracována.

Sedmivrstvý model ISO/OSI je zobrazen v tabulce 4.2, kde je porovnáván s modelem TCP/IP.

4.1.3 Síťový model TCP/IP

Síťový model TCP/IP (Transmission control protocol / internet protocol) je dnes podporován ve většině sítí a zařízení. Detaily protokolů využívaných v tomto modelu jsou uváděny v RFC dokumentech (Request for comments [29]). Podobně, jako u modelu ISO/OSI, tak i zde je komunikace rozdělena do více vrstev, konkrétně do čtyř. Tabulka 4.2 ukazuje vrstvy obou modelů a jejich vzájemnou podobnost. V krátkosti se budu věnovat popisu jednotlivých vrstev modelu TCP/IP [3].

Model ISO/OSI	**Model TCP/IP**
Aplikační vrstva	Aplikační vrstva
Prezentační vrstva	
Relační vrstva	
Transportní vrstva	Transportní vrstva
Síťová vrstva	Internetová vrstva
Spojová vrstva	Vrstva síťového rozhraní
Fyzická vrstva	

Tabulka 4.2: Referenční model ISO/OSI v porovnání s modelem TCP/IP

Aplikační vrstva

Aplikační vrstva poskytuje své služby běžící aplikaci. Vytváří tak rozhraní mezi aplikací a sítí, což vede k nezávislosti aplikace nad komunikačním médiem. Jednotlivá zařízení komunikující v rámci aplikační vrstvy si předávají informace v podobě hlavičky aplikační vrstvy, za kterou mohou následovat data aplikace.

Aplikační vrstva modelu TCP/IP zahrnuje hned tři vrstvy modelu ISO/OSI. Stará se tak i o navázání a ovládání komunikace. Vyjednává datový formát a předává aplikaci data tak, aby s nimi mohla pracovat jako s nepřerušovaným proudem.

Nad aplikační vrstvou je definován nespočet protokolů, tím asi nejznámějším je je protokol HTTP (Hypertext transfer protocol).

Transportní vrstva

Nad transportní vrstvou jsou definovány pouze dva protokoly. Protokol TCP (Transmission control protocol) a protokol UDP (User datagram protocol). Transportní vrstva poskytuje své služby vyšší vrstvě a tyto služby přímo plynou z vlastností protokolů TCP nebo UDP.

Protokol TCP zajišťuje spolehlivé doručení dat příjemci. Používá metodu potvrzování přijatých dat a v případě, kdy potvrzení nedorazí, data odešle znovu. Vzhledem k vyšší režii se tento protokol nehodí pro přenášení objemných dat, kde je lépe použít protokol UDP.

Protokol UDP na rozdíl od protokolu TCP nezajišťuje spolehlivé doručení. Neposílá tak potvrzení a ani se nestará o znovu poslání nedoručených dat. Na druhou stranu vyniká vyšší rychlostí a jednoduchostí. Využívají ho služby, jako jsou DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) apod.

Internetová vrstva

Nad internetovou vrstvou pracuje především protokol IP (Internet protocol). Umožňuje rozlišovat jednotlivá zařízení v sítí dle jejich unikátní adresy a stará se o směrování dat v síti. V současnosti je převážně používán protokol IP verze 4, který definuje 32 bitové adresy zařízení. Z důvodu omezeného počtu adres je definován protokol IP verze 6, který mimo 128 bitové adresy přináší také bezpečnostní vylepšení.

Dalším protokolem nad internetovou vrstvou je například ARP (Address resolution protocol). Ten pomocí známé IP adresy hledá MAC adresu patřičného zařízení v síti. Žádost ARP je s vyplněnou IP adresou poslaná všem účastníkům v síti a ten, který je v adrese uveden vyplní svoji MAC adresu a odesílateli odpoví. Obráceně pracuje protokol RARP (Reverse address resolution protocol), který hledá IP adresu pomocí známé MAC adresy.

Vrstva síťového rozhraní

Vrstva síťového rozhraní definuje protokoly a hardwarové prostředky nutné pro doručení dat přes komunikační médium. V rámci této vrstvy je definován například standard Ethernet, viz kapitola 4.1.1.

4.1.4 Popis vlastností ethernetového řadiče ENC28J60

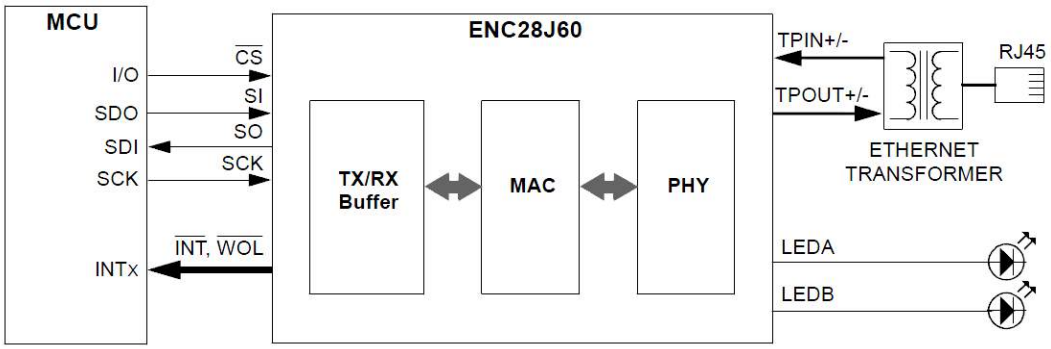
Masivní rozšířenost standardu IEEE 802.3 postřehla také firma Microchip Technology a vyvinula integrovaný obvod ENC28J60, který slouží jako řadič rozhraní Ethernet a je s ním plně kompatibilní [7]. Pro komunikaci s řídícím mikrokontrolérem je vybaven synchronní sériovou sběrnicí SPI (Serial peripheral interface), která je založena na čtyřech vodičích. Obvod není od výrobce vybaven svoji vlastní MAC adresou. Je nutné ji nastavit až za běhu aplikace programově.

Je dodáván ve 28 vývodovém pouzdře SOIC (small-outline integrated circuit) určeném pro SMT montáž (surface mount technology). Obsahuje výstupy pro indikační LED diody, které lze nastavit pro signalizaci síťového provozu nebo mohou být volně konfigurovatelné. Pro svoji funkčnost vyžaduje napájení 3,3V, krystal o kmitočtu 25MHz, několik diskrétních součástek a konektor RJ45 s integrovanými pulsními transformátory [28].

Obsahuje vyrovnávací paměť o velikosti 8kB pro příchozí a odchozí pakety. Nabízí rozsáhlé možnosti konfigurace filtrování a odmítání paketů, výpočet CRC kontrolních součtů a nastavitelný přerušovací podsystém. Pro přímou komunikaci přes fyzické médium je vybaven fyzickou vrstvou (PHY - physical layer) zajišťující správný převod digitálního signálu na analogový a obráceně. Protokol IEEE 802.3 je implementován ve vrstvě MAC. Blokové schéma typického použití tohoto obvodu ukazuje obrázek 4.1.

Přehled vybraných vlastností obvodu ENC28J60:

- Dodáván v 28 vývodovém SOIC pouzdře.
- Provozní teplota -40°C – +85°C.
- Pracovní kmitočet 25MHz, výstupní hodinový signál s nastavitelnou předděličkou.
- Napájení 3,14V – 3,45V DC, proudový odběr nejvýše 250mA.
- Komunikace s mikrokontrolérem přes rozhraní SPI.



Obrázek 4.1: Blokové schéma typického použití obvodu ENC28J60 [7]

- Konfigurace obvodu přes řídící registry.
- Kompatibilní s protokolem IEEE 802.3
- Interní DMA (direct memory access) řadič pro rychlejší datové přesuny.
- Sedm nastavitelných zdrojů přerušení.

4.2 Technologie rozhraní USB

Historie rozhraní USB se začala psát v roce 1994 s myšlenkou jednodušeji připojit externí zařízení k počítači. Do té doby se používalo zejména sériové rozhraní RS-232, které bylo limitováno svoji přenosovou rychlostí a bylo možné k němu v jedem okamžik připojit pouze jedno zařízení. První specifikace USB 1.0 byla představena v roce 1996 a byla plně kompatibilní se standardem Plug&Play. Bylo tím umožněno připojit externí zařízení i za běhu počítače. Operační systém zařízení rozpozná a pokusí se zavést dostupný ovladač. Zařízení je také možno za běhu odpojit [45].

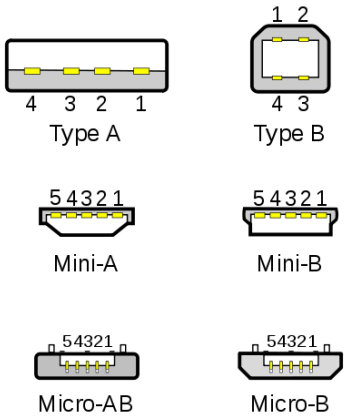
Rozhraní USB se však masivně rozšířilo až o dva roky později, kdy byl schválen standard USB 1.1. Ten umožnil komunikovat se zařízením na dvou rychlostních úrovních. Pomalá zařízení (například ovladače, myši nebo klávesnice) mohli pracovat s rychlostí 1,5Mb/s. Rychlejším zařízením (například externím diskům) bylo umožněno pracovat s datovým přenosem až 12Mb/s.

Do dnešního dne byly postupně představeny dvě zpětně kompatibilní specifikace rozhraní USB. USB 2.0 zvýšila rychlost přenosu až k 480Mb/s a USB 3.0 přineslo nový konektor a také došlo ke zvýšení rychlosti až 5Gb/s. Další popis bude věnovaný standardu USB 2.0 případně 1.1.

4.2.1 Mechanické a elektrické vlastnosti

Rozhraní USB obsahuje čtyři vodiče. Po dvou je přenášeno napájecí napětí 5V omezené nejvyšším proudovým odběrem 500mA. Zbylé dva vodiče tvoří kroucenou, diferenciální dvoulinku pro snížení rušení. Maximální délka vodiče je omezena na 5m. Externí zařízení může být volitelně napájeno přímo z rozhraní USB. Běžně je napájení omezenou proudem do 100mA, pokud však zařízení potřebuje vyšší proudový odběr, na jeho žádost je mu umožněno odebírat až 500mA [16].

Standard definuje konektory dvou druhů. Typ A a typ B a z nich vycházející minimalizované varianty, viz obrázek 4.2. Význam jednotlivých vodičů je uveden v tabulce 4.3.



Obrázek 4.2: Typy konektorů rozhraní USB 2.0 [45]

Číslo pinu	Konektor standardní		Konektor mini/micro	
	Popis	**Barva vodiče**	**Popis**	**Barva vodiče**
1	+5V	Červená	+5V	Červená
2	Data –	Bílá	Data –	Bílá
3	Data +	Zelená	Data +	Zelená
4	Nulový potenciál	Černá	nezapojen	—
5	—	—	Nulový potenciál	Černá

Tabulka 4.3: Označení a význam vodičů rozhraní USB 2.0

4.2.2 Topologie rozhraní USB

K rozhraní USB je možné připojit zařízení dvojího druhu. Koncová zařízení, která jsou schopna přijímat nebo vysílat data a rozbočovače (anglicky hub), které převádí jeden přípojný bod na více přípojných bodů. V topologii sběrnice USB je v nejvyšší úrovni kořenový rozbočovač, ke kterému lze připojit další rozbočovače nebo přímo koncová zařízení.

Připojením rozbočovače rozšíříme topologii o jednu úroveň. Těchto úrovní je možné vytvořit nejvýše sedm, tedy můžeme za sebe připojit nejvýše šest rozbočovačů. Celkový počet zařízení, které může obsluhovat jedna sběrnice USB je 127.

4.2.3 Typy datových přenosů

Tato podkapitola byla volně převzata z [16].

Mezi koncovým zařízením a počítačem probíhá datový přenos čtyřmi odlišnými způsoby. S vysokou prioritou pracují řídící dotazy, které slouží k řízení nastavení a řízení koncového zařízení. Při komunikaci je automaticky hlídána detekce chyb.

Zařízení, která periodicky posílají malé množství dat (například myš nebo klávesnice) komunikují v režimu přenosu při přerušení. Počítač se v pravidelných intervalech dotazuje koncového zařízení na nová data. Pokud jsou k dispozici, koncové zařízení je odešle.

V hromadném přenosu komunikují ty zařízení, které přenáší vyšší množství dat a požadují jejich spolehlivost. Rychlost přenosu se řídí dle vytížení sběrnice a během něj je kontrolována správnost dat. Typickým zařízením, které komunikuje v hromadném režimu je například tiskárna.

Posledním typem datového přenosu je izochronní přenos. V tomto režimu se přenáší vyšší množství dat, na které je požadavek omezeného zpoždění a konstantního datového toku po celou dobu přenosu. V případě chybného doručení není požadavek na jeho opravu. Nejčastěji se takto přenáší data pro zvukové zařízení.

4.2.4 Popis vlastností obvodu FT2232D

Připojit vestavěný systém k počítači přes rozhraní USB lze pomocí integrovaného obvodu FT2232D od firmy FTDI (Future technology devices international Ltd) [8]. Tento obvod slouží jako převodním mezi sběrnicí USB a asynchronním rozhraním UART. Řídící mikroprocesor je tak plně odstíněn od problematiky rozhraní USB a velice snadno si vyměňuje data s počítačem.

Obvod FT2232D je dodáván ve 48 vývodovém LQFP (Low-profile Quad Flat Package) pouzdře určeném pro SMT montáž. Externí EEPROM paměť (Electrically Erasable Programmable Read-Only Memory) lze připojit k převodníku a získat tím možnost individuálního nastavení USB rozhraní. V externí paměti můžou být uložena vlastní data pro identifikaci zařízení, například USB VID (vendor identification - identifikace výrobce), PID (product identification - identifikace výrobku), sériové číslo a popis výrobku.

Převodník je také vhodný do vestavěných systémů, které jsou napájeny z vlastního zdroje nebo jsou napájeny z rozhraní USB. Pro správnou funkci vyžaduje napájení 5V, krystal pracující na kmitočtu 6MHz a několik diskrétních součástek.

V operačním systému počítače lze s obvodem pracovat pomocí dvou typů ovladačů. Při použití ovladače VCP (virtual com port) je připojené zařízení bráno počítačem jako virtuální sériový port, z kterého lze jednoduše číst i zapisovat. Obvod FT2232D je v tomto případě pro obě komunikační strany transparentní.

Druhý ovladač, který lze použít je označován jako D2XX. Tento ovladač umožňuje přímí přístup k obvodu FT2232D a jeho konfiguraci. Ovladač D2XX nabízí speciální API rozhraní pro nastavení parametrů obvodu a umožňuje také zápis dat do externí EEPROM paměti. Bližší informace o ovladačích lze získat v [9].

Přehled vybraných vlastností obvodu FT2232D:

- Dodáván ve 48 vývodovém LQFP pouzdře.
- Provozní teplota -40°C – +85°C.
- Pracovní kmitočet 6MHz.
- Napájení 4,35V – 5,25V DC, proudový odběr 30mA.
- Komunikace s mikrokontrolérem přes rozhraní UART.
- Konfigurace obvodu v externí EEPROM paměti.

- Dva nezávislé komunikační kanály.
- Kompatibilní s protokolem USB 2.0 s rychlostí 12Mb/s.

Kapitola 5

Návrh vlastního zabezpečovacího systému

V této kapitole se čtenář seznámí s koncepcí vlastního zabezpečovacího zařízení. V následujícím textu budou zmíněny jeho klíčové vlastnosti, rozdělení celého zařízení do více samostatných bloků a výběr vhodných komponent.

5.1 Vlastnosti navrženého systému

Ze získaných poznatků v oblasti zabezpečovací techniky jsem navrhl cílové vlastnosti, které by hotové zařízení mělo splňovat. Při jejich definování jsem vycházel ze svých zkušeností a inspiroval jsem se profesionálními produkty od firem Jablotron [15] nebo Paradox [26].

Pocit bezpečí

Všechna zabezpečení jsou za jistých okolností překonatelná. Vlastní zabezpečovací systém je tedy s touto myšlenkou od počátku navrhován. Základním cílem není vytvořit zařízení, které nebude možné žádným způsobem překonat. Základním cílem je vytvořit takové zařízení, které poskytne uživateli významný pocit bezpečí a bude ho chránit před většinou běžných nebezpečí.

Snadné ovládání

Malou rozšířenost EZS má na svědomí mimo pořizovací ceny i jejich složité každodenní ovládání. Zejména senioři se pomalu učí pracovat s moderními a pro ně složitými věcmi. Navrhuji takové zařízení, které nebude uživatele omezovat jedním způsobem ovládání. Uživatel si bude moci zvolit takový způsob, který mu bude nejvíce vyhovovat. Například identifikace pomocí bezkontaktní čipové karty (technologie RFID, kapitola 3.3), heslo zadávané přes numerickou klávesnici, SMS zprávou nebo hovorem z mobilního telefonu.

Pro zvýšení bezpečnosti se nabízí myšlenka kombinace různých způsobů ovládání. Identifikace uživatele přiložením čipové karty a následné zadání hesla. Nebo v obsahu SMS zprávy uvést příkaz pro zabezpečovací systém doplněný vlastním heslem.

Univerzálnost

Nikdy nemůžeme říci, že nebezpečí, které neznáme dnes, nebudeme znát ani zítra. Schopnost připojit k systému různé druhy čidel je velice významnou vlastností. Připojit prvky plášťové, prostorové a požární ochrany, stejně jako prvky tísňového hlášení by měli být naprostou samozřejmostí. V případě speciálních čidel (například měření teploty, vlhkosti apod) by měl systém nabízet takové prostředky, které by neznemožňovali jejich připojení.

Vysoké množství připojitelných čidel

Vytvořit zabezpečovací zařízení, které umožňuje připojit pevně definovaný počet čidel není mým záměrem. Zařízení by v případě potřeby mělo nabízet možnosti, jak rozšířit jejich počet. Realisticky však uznávám, že není možné připojit neomezené množství senzorů. Na druhou stranu, by jich měl systém nabídnout tolik, aby pokryli i potřeby náročných uživatelů. Nezávislé rozlišení jednotlivých čidel je v tomto případě neoddiskutovatelným faktem.

Odolnost proti výpadku elektrické energie

Při přerušení dodávky elektrického proudu do domácnosti bude zabezpečovací zařízení schopné pracovat ze svého záložního zdroje. Nenastane situace, že při krátkodobém výpadku přestane být domácnost střežena. Uživatel by měl být také na tuto situaci náležitě upozorněn, například formou SMS zprávy. Může se totiž jednat jak o závadu způsobenou proudovým přetížením jističů, tak o úmyslné napadení domácnosti.

Upozornění na hrozbu více způsoby

Zařízení bude umožňovat uživateli zvolit vhodný způsob, kterým bude chtít upozornit na různé bezpečnostní hrozby. Ideálně se zařízení nebude spoléhat na ohlášení poplachu pouze jedním způsobem, nýbrž je bude kombinovat. Například místní upozornění pomocí optické a akustické signalizace probíhající současně na více místech s kombinací vzdáleného upozornění na mobilní telefon.

Vzdálený přenos poplachu dovoluje informovat současně více uživatelů, včetně bezpečnostní agentury přes PCO, viz kapitola 2.3.5. Připojením zabezpečovacího systému k internetu můžeme informace přenášet také prostřednictvím elektronické pošty.

Inteligentní domácnost

Schopnost upozornit na bezpečnostní hrozbu je v mnoha případech dostačující, avšak schopnost hrozbě zabránit je o poznání užitečnější. Automatická reakce na únik plynu, která povede k jeho uzavření, tak může zachránit nejen hodnotný majetek, ale i daleko cennější lidský život.

Preventivní opatření mohou odradit případného zloděje. Rozsvícení osvětlení v domácnosti a jejich zhasínání budí iluzi lidské přítomnosti i v jinak zcela prázdné domácnosti. Stejný účinek má například i zapnutá televize.

Zařízení bude umožňovat připojit a dvoustavově ovládat libovolný elektrospotřebič v domácnosti. Počínaje hlásiči poplachu, osvětlením, garážovými vraty a konče elektrickými uzávěry plynu nebo vody. Každé připojené zařízení bude možné ovládat vzdáleně a automaticky dle předem nastaveného časového plánu nebo při splnění definovaných podmínek.

Manuální ovládání připojených zařízení nebude ovlivněno, případně bude ovládáno přes zabezpečovací systém. Pokud by takové řešení nebylo možné, bude zařízení nabízet ovládání jednoho elektrospotřebiče dvěma výstupy. Jeden výstup bude zapojen paralelně a druhý sériově k vypínači.

Vzdálený dohled

Mít neustále přehled o dění v domácnosti je velice příjemnou vlastností EZS. Na mobilní telefon je možné dostávat pravidelná hlášení nebo být pouze informován o vybraných událostech. Protože je dnes internet stejně rozšířený jako mobilní telefon, tak zařízení bude využívat i této technologie. Rozšíří se tím možnosti využití vzdáleného dohledu a ovládání domácnosti.

Archivace všech zaznamenaných událostí

Zejména pro zpětnou kontrolu nebo odhalení závady bude sloužit archivace všech zaznamenaných událostí. Uživatel nebo servisní technik tak bude moci vysledovat postup, který vedl k nefunkčnosti systému. Při napadení domácnosti zlodějem bude možné díky archivu velice přesně vysledovat jakým způsobem došlo k vniknutí do domácnosti, co přesně tam zloděj dělal a kde se pohyboval.

Snadná oprava poškozeného zařízení

Každá součástka má svoji životnost a občas se stane, že se něco porouchá. Navrhovaný zabezpečovací systém by měl při svém poškození být snadno opravitelný, případně by neměl znemožnit výměnu poškozené části.

5.2 Blokové schéma

Pro dodržení výše uvedených vlastností jsem navrhl distribuovaný systém, který je v základní variantě složen ze čtyř modulů. Komunikace mezi nimi probíhá bezdrátově.

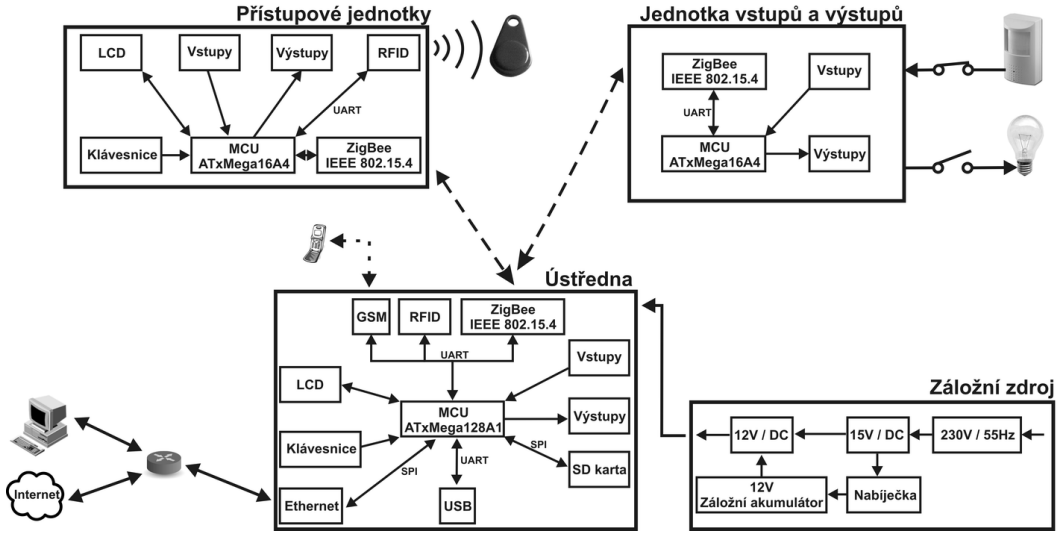
Bezdrátová komunikace

Zvolením bezdrátové komunikace zajišťuji, že bude možné systém velice snadno nainstalovat do domácnosti. Vyhneme se potřebě použít značné množství kabeláže, která by jinak sloužila pouze pro komunikaci mezi jednotlivými moduly. Velmi kladnou vlastností bezdrátového systému je také jednoduchost jejího případného rozšíření. Při použití vhodného komunikačního protokolu nebude složité do systému přidat zcela nový prvek.

Bezdrátová komunikace bude probíhat pomocí protokolu ZigBee definovaného nad standardem IEEE 802.15.4, viz kapitola 3.2. Tento druh komunikace je do jisté míry velmi spolehlivý, zejména také proto, že podporuje šifrování.

Distribuovaný systém

V mém případě je zabezpečovací zařízení složeno ze tří samostatných modulů a záložního zdroje. Důvodem proč jsem zvolil toto řešení je jeho univerzálnost. Každá část systému se stará o svoji práci a v případě potřeby si přes jednotné komunikační rozhraní vyměňuje informace s dalšími moduly.



Obrázek 5.1: Blokové schéma vlastního EZS

Tento přístup umožňuje se snáze vypořádat s nefunkčností některého z prvků. Při poruše je pak především finančně výhodnější a časově rychlejší vyměnit nefunkční modul, než celý systém.

Ústředna

Žádný EZS se nemůže obejít bez své ústředny, viz kapitola 2.3.1. Výjimkou tak není ani vlastní zabezpečovací systém. Ústřednu jsem navrhl s myšlenkou, aby byla schopna pracovat zcela samostatně a nemusela se spoléhat na přítomnost dalších modulů.

Vycházím zejména ze skutečnosti, že v malých domácnostech nebo víkendových chatách je bezdrátový EZS příliš finančně nákladný. V malých objektech, kde není zapotřebí připojovat vysoké množství čidel, se tak stává ústředna jediným prvkem zabezpečovacího zařízení. Avšak v mém návrhu tím uživatele v žádném případě neomezuji. Ústředna obsahuje všechny důležité komponenty k tomu, aby i samostatně nabízela veškerou funkcionalitu zmíněnou v kapitole 5.1.

Do ústředny je zahrnuta kompletní přístupová jednotka s klávesnicí, displejem a čtečkou RFID pro bezkontaktní identifikaci. Je vybavena GSM modulem, přes který komunikuje s mobilním telefonem. K počítači ji lze připojit přes rozhraní Ethernet nebo USB. Svými výstupy dovede ovládat připojené elektrospotřebiče a provádí také archivaci všech zaznamenaných událostí na vloženou paměťovou SD (Secure digital) kartu.

Ústřednu je možné zařadit do kategorie smíšeného typu. Konkrétně kombinuje vlastnosti všech druhů ústředen, protože je vybavena připojením smyčkových a přímo adresovatelných bezdrátových čidel.

Přístupová jednotka

Přístupová jednotka slouží k ovládání běžných činností zabezpečovacího systému. Nejčastěji ji bude uživatel využívat v situaci, kdy odchází nebo přichází domů, za účelem zapnutí nebo vypnutí střežení domácnosti. Způsob jakým bude uživatel tyto činnosti vykonávat by ho

neměl zbytečně omezovat. Toho bych chtěl dosáhnout zejména tím, že si uživatel zvolí takové ovládání, které mu bude příjemné.

Přístupová jednotka je vybavena čtečkou RFID karet, čímž umožňuje uživateli velice snadné a rychlé zapnutí nebo vypnutí střežení. Bude k ní také připojena numerická klávesnice, kterou bude uživatel schopen zadat své heslo a ovládat jednotku. Informace pro interakci s uživatelem budou zobrazovány na LCD (Liquid crystal display) displeji.

Dále bude jednotka sloužit k základním administrativním úkonům bez použití počítače nebo mobilního telefonu. Bude s ní možné nahlížet do archívu zaznamenaných aktivit, přerušit probíhající poplach, omezit práva jednotlivých uživatelů nebo prohlížet aktuální stav jednotlivých čidel a připojených elektrospotřebičů.

Uvažuji použití přístupové jednotky u všech vchodových dveří do domácnosti. K odblokování střežení nebude uživatel omezován nutností použít vždy stejný vchod.

Jednotka vstupů a výstupů

Navržený zabezpečovací systém bude nabízet prostřednictvím jednotky vstupů a výstupů snadné možnosti rozšíření připojitelných čidel a elektrospotřebičů. Tato jednotka bude obsahovat pouze vyhodnocovací obvody smyčkových čidel a dvoustavové výstupy pro ovládání připojených zařízení.

Zabezpečovací systém nebude nijak omezovat množství těchto jednotek. Jediné omezení bude způsobeno implementační náročností a paměťovými možnosti cílového mikrokontroléru. Bude však možné připojit nejméně pět jednotek vstupů a výstupů.

Záložní zdroj

Pro případ výpadku elektrické energie bude zabezpečovací systém vybaven záložním zdrojem. Ten bude systém napájet ze svého olověného akumulátoru. Spotřeba zálohovaných částí systému a jmenovitá hodnota kapacity akumulátoru pak budou určovat maximální časový úsek, po který bude záložní zdroj schopen plnit svůj účel.

Záložní zdroj bude obsahovat inteligentní nabíječku olověných akumulátorů. Funkce nabíječky bude zejména optimální kontrola maximální kapacity a životnosti akumulátoru. Nabíječka bude automaticky volit takové nabíjecí cykly, které nebudou poškozovat akumulátor a zároveň umožní jeho rychlé nabití na plnou úroveň.

V případě potřeby výměny akumulátoru za jiný kus, který má odlišnou jmenovitou hodnotu své kapacity, bude možné nabíječku přenastavit pro správné nabíjení nově vloženého akumulátoru.

5.3 Výběr vhodné platformy

Navržený EZS je složen ze tří modulů řízených mikrokontrolérem. Zejména modul ústředny obsahuje vysoký počet periferií, se kterými je nutné komunikovat pomocí definovaného rozhraní. Velice důležitým krokem při návrhu se stal výběr vhodné platformy mikrokontrolérů.

Chtěl jsem dodržet v celém systému určitou jednotnost a ve všech modulech použít mikrokontroléry od jedné firmy. Ideálně mikrokontroléry stejné architektury. Zaměřil jsem se proto na relativně novou rodinu mikrokontrolérů ATxMega od firmy Atmel. Stručným popisem zvolené rodiny bude pokračovat následující text.

Rodina mikrokontrolérů ATxMega

V roce 2008 firma Atmel představila novou rodinu 8 bitových mikrokontrolérů ATxMega založených na jádře AVR RISC. Tato rodina je rozdělena do tří skupin, které se liší počtem pinů použitého pouzdra a počtem periferií. Nejvybavenější skupina je označována jako A1 a je dodávána ve 100 vývodovém TQFP (Thin quad flat pack) pouzdře určeném pro SMT montáž. Střední kategorie je označena koncovkou A3, dodávána je v 64 vývodovém TQFP pouzdře. Nejnižší skupina je značena koncovkou A4, která se vyrábí ve 44 vývodovém TQFP pouzdře.

Potřebám ústředny nejlépe vyhovuje mikrokontrolér ze skupiny A1. U nás je v kusovém množství dostupný typ s pamětí programu 128kB, který je označován jako ATxMega128A1.

Přehled vybraných vlastností obvodu ATxMega128A1:

- 8b mikrokontrolér s RISC jádrem AVR
- Dodáván ve 100 vývodovém TQFP pouzdře.
- Provozní teplota -40°C – +85°C.
- Pracovní kmitočet 0 – 32MHz.
- Napájení 2,7V – 3,6V DC, proudový odběr 10mA při pracovním kmitočtu 12MHz
- 128kB paměti programu, 8kB interní SRAM paměti (Static random access memory) a 2kB interní EEPROM paměti
- 78 I/O pinů, 8 x 16b čítač/časovač, 8 x sériové rozhraní UART, 4 x sériové rozhraní SPI
- Programování přímo v aplikaci přes rozhraní PDI (Program and debug interface)
- Hardwarová podpora šifrování

Bližší informace o mikrokontrolérech ATxMega v katalogovém listu výrobce [1].

Kapitola 6

Hardwarová realizace

V této kapitole budou diskutovány návrhy schémat elektroniky zabezpečovacího systému společně s návrhem a osazením desek plošných spojů. Čtenář bude seznámen s řešením problému, na které jsem během práce narazil. Zmíněny budou také elektrické a mechanické vlastnosti celého systému.

Seznam všech použitých součástek je uveden v příloze a na přiloženém CD.

6.1 Napájení jednotlivých modulů

Zabezpečovací systém využívající moderních technologií si žádá také moderní zdroj určený pro jeho napájení. Lineární stabilizátory napětí pomalu ustupují před jednoduchými spínanými, kteří vynikají svojí vysokou účinností. Cenově jsou také dostupné a proto jsem v celé aplikaci zvolil použití spínaných stabilizátorů.

6.1.1 Princip spínaného stabilizátoru

Pro zjednodušení si představme spínaný zdroj tvořený přepínacím prvkem, cívkou a kondenzátorem, viz obrázek 6.1a. Takový zdroj pak pracuje ve dvou fázích [35]:

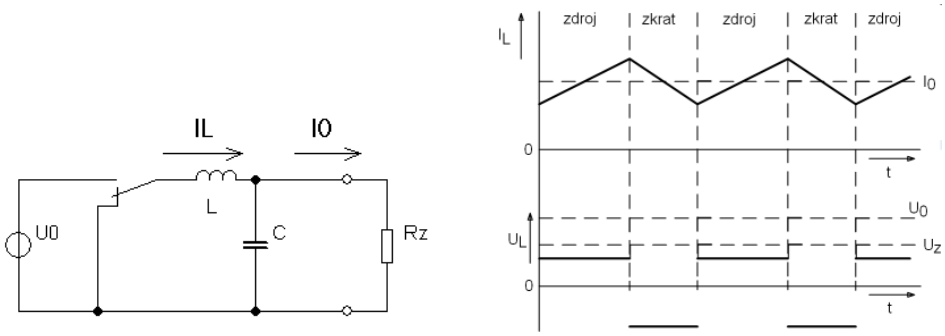
- Cívka je připojena ke zdroji napětí.
  Na cívce vzniká úbytek napětí roven rozdílu potenciálů mezi jejími konci. Proud cívkou stoupá, čímž roste energie akumulovaná v magnetickém poli jádra cívky. V idealizovaném případě lze považovat nárůst proudu za lineární, viz obrázek 6.1b. Kondenzátor akumuluje náboj odpovídající ploše trojúhelníka pod grafem proudu cívkou, čímž snižuje kolísání napětí na výstupu.

- Cívka je zkratována na nulový potenciál
  Po odpojení cívky od zdroje napětí získává zátěž energii z magnetického pole cívky. Proud cívkou v idealizovaném případě klesá lineárně a kondenzátor dodává do zátěže energii rovnou ploše trojúhelníka pod grafem proudu cívkou, viz obrázek 6.1b.

Výstupní napětí je dáno střídou přepínání mezi jednotlivými stavy, viz následující vztah.

$$U_z = U_0 * \frac{t_{on}}{T} \quad [V, V, s, s]$$

kde U_z značí výstupní napětí, U_0 značí vstupní napětí, t_{on} značí dobu připojení cívky ke zdroji napětí a T označuje periodu spínání.



(a) Zjednodušené schéma [35] (b) Průběh proudu a napětí [35]

Obrázek 6.1: Princip spínaného stabilizátoru

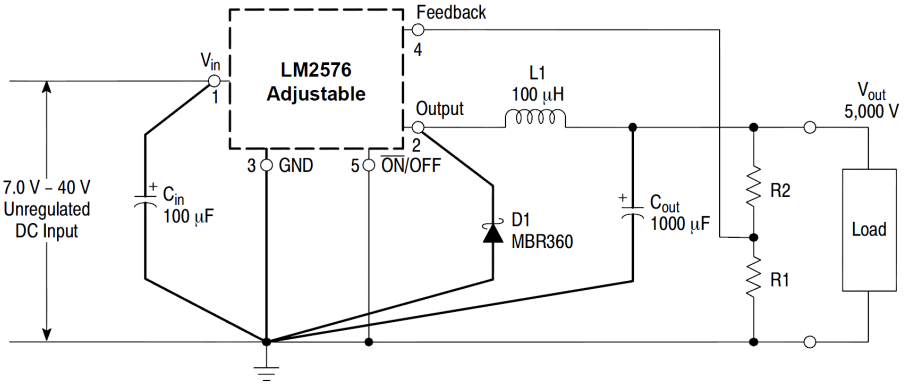
6.1.2 Spínaný stabilizátor LM2576

Snadno použitelným a cenově dostupným spínaným stabilizátorem je obvod LM2576 od firmy ON Semiconductor [19]. Je dodáván ve variantě pevně nastaveného stabilizátoru s výstupním napětím 3,3V, 5V, 12V a 15V. Také je dodáván ve variantě libovolně nastavitelného stabilizátoru. V obou variantách nabízí výstupní proud až 3A a účinnost téměř 90%. Pro svoji správnou funkci vyžaduje jen nezbytné diskrétní součástky. Doporučené zapojení výrobcem je uvedeno na obrázku 6.2.

Výstupní napětí je regulováno poměrem rezistorů R_1 a R_2 a je dáno vztahem:

$$V_{out} = V_{ref}\left(1 + \frac{R_2}{R_1}\right) \quad [V, V, \Omega, \Omega]$$

kde V_{out} označuje výstupní napětí a $V_{ref} = 1{,}23$.



Obrázek 6.2: Doporučované zapojení výrobce [19]

Všechny moduly zabezpečovacího zařízení jsou napájeny právě tímto spínaným stabilizátorem. Ať už ve variantě s pevným napětím 5V nebo v nastavitelné variantě.

6.2 Ústředna EZS

6.2.1 Schéma zapojení elektroniky

Schéma zapojení elektroniky, stejně jako návrh desek plošných spojů (dále jen „DPS“), jsem navrhoval v prostředí programu Eagle verze 5.6.0. Tento program nabízí přívětivé uživatelské rozhraní a usnadňuje tím samotný návrh aplikace. Obsahuje mimo editor schémat a DPS také editor součástek.

Výsledné schéma zapojení elektroniky je uvedeno v příloze nebo na přiloženém CD.

Řídící mikrokontrolér

Hlavním členem ústředny je mikrokontrolér ATxMega128A1 (IC_4), který byl detailněji popsán v kapitole 5.3. Zapojen je dle doporučení výrobce [1]. Zejména je nutné dodržet připojení všech napájecích a zemnících pinů, které jsou doplněny nejméně čtyřmi keramickými kondenzátory ($C_{15} - C_{18}$) s kapacitou 100nF. Protože je mikrokontrolér vybaven vnitřním generátorem hodinového taktu, tak není nutné použít externí krystal.
K programování mikrokontroléru slouží rozhraní PDI, které se připojí konektorem K_{25}. Za použití programátoru doporučeným výrobcem je možné nahrát program do cílového mikrokontroléru přímo v aplikaci.

Napájení

Periferní obvody jsou ve větší míře napájeny stejným napětím jako mikrokontrolér, tedy 3,3V. Jsou však použity i takové obvody, které pro svoji funkci vyžadují napětí 5V. Jmenovitě se jedná o obvody FT2232D (IC_5) s pamětí EEPROM (IC_6, viz kapitola 4.2.4), čtečka RFID karet ID12 (IC_7, viz kapitola 3.3.2) a alfanumerický LCD displej.

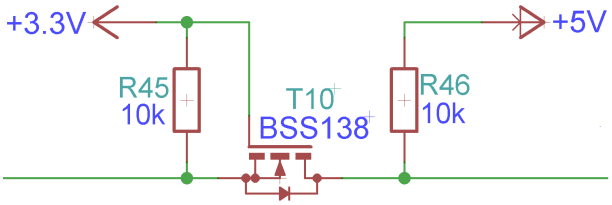
S ohledem na rozměry a jednoduchost zapojení je použit spínaný stabilizátor LM2576 (IC_1) s pevným napětím 5V. Napětí 3,3V je získáno za použití lineárního stabilizátoru LF33CDT (IC_3) [18]. Jeho výhodou je, že nepotřebuje mimo filtračních kondenzátorů žádné další součástky. Pracuje s maximálním proudem 500mA, což dostačuje k napájení patřičných obvodů. Konkrétně mimo mikrokontroléru i Ethernetového řadiče ENC28J60 (IC_2, viz kapitola 4.1.4), modulu pro bezdrátovou komunikaci XBee (IC_8, viz kapitola 3.2.4) a paměťovou SD kartu (K_30).

Přizpůsobení napěťových úrovní na sběrnici

Různé napěťové úrovně mezi mikrokontrolérem a připojenými periferii způsobují významný problém. Mikrokontrolér nemá téměř žádnou toleranci k napětí na jeho pinech. Jakékoli napětí vyšší o 0,5V než je jeho napájecí napětí povede k destrukci samotného vývodu nebo i celého mikrokontroléru. Musíme tedy vyřešit přizpůsobení těchto napěťových úrovní. A aby to nebylo příliš snadné, tak je nutné zachovat propustnost v obou směrech.

Řešení, jak napěťově přizpůsobit obousměrnou komunikační sběrnici, zveřejnila firma NXP ve své aplikační poznámce AN10441 [24]. Firma NXP je tvůrcem sběrnice I2C a řešila stejný problém jako já. Proto navrhla důvtipné zapojení MOSFET tranzistoru (Metal oxide semiconductor field effect transistor) s indukovaným kanálem typu N, viz obrázek 6.3. Hradlo tranzistoru je připojeno k nižšímu napětí, emitor je přes pull-up rezistor zapojen na sběrnici s nižším napětím a kolektor je přes pull-up rezistro připojen na sběrnici s vyšším napětím.

V situaci, kdy jsou obě zařízení ve stavu vysoké logické úrovně, je tranzistor uzavřen a obě strany sběrnice jsou odděleny. Pokud zařízení s nižším napětím přejde do stavu logické nuly, způsobí tak otevření tranzistoru, což povede k uzemnění druhé strany sběrnice. Když zařízení na straně s vyšším napětím přejde do stavu logické nuly, tak přes vnitřní diodu MOSFET tranzistoru dojde k uzemnění opačné strany sběrnice [24].



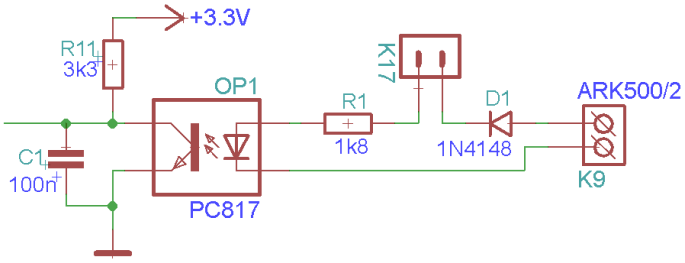
Obrázek 6.3: Přizpůsobení napěťových úrovní na sběrnici

Řešení vstupní smyčky

Požadavek připojit různé druhy čidel vedl k problematice návrhu vhodného vstupního obvodu. Obvod musí být schopen oddělit připojené čidlo od mikrokontroléru ve snaze jej ochránit před případným zničením.

Řešení spočívá ve vhodně zapojeném optočlenu, čímž dojde ke galvanickému oddělení a tím k ochraně před vysokým napětím nebo přepólováním. Obvod je možné doplnit signalizační LED diodou, která poslouží pro rychlé zjištění stavu vstupu. Pokud nebude LED dioda použita, je nutné ji nahradit zkratovací propojkou.

Připojením napětí 12V dojde k rozsvícení LED diody uvnitř optočlenu. Produkované záření diody způsobí otevření fototranzistoru, což povede k uzemnění jeho kolektoru a mikrokontrolér tak vyhodnotí stav logické nuly.

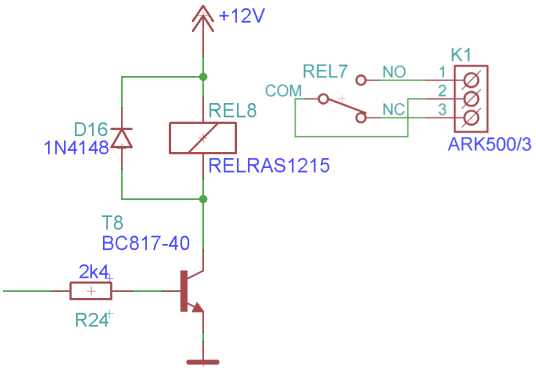


Obrázek 6.4: Vstupní obvod

Řešení výstupní smyčky

Připojené elektrospotřebiče je dle specifikace vlastností nutné ovládat způsobem zapnuto/vypnuto. Aby bylo možné spínat spotřebiče různě napájené a různých proudových odběrů je použito řešení s elektromagnetickým relé. K cívce relé je paralelně připojená usměrňovací dioda, která slouží jako filtrace indukovaného napětí při ovládání relé.

Relé je dimenzováno proudem 15A a je spínáno jmenovitým napětím 12V. Spotřeba sepnutého relé je 30mA.



Obrázek 6.5: Výstupní obvod

6.2.2 Návrh DPS a osazení součástkami

Některé součástky použité v návrhu elektroniky jsou dostupné pouze v provedení pro povrchovou montáž. Proto jsem se v celém návrhu snažil o upřednostnění těch součástek, které jsou dodávány v pouzdře typu SMD (Surface mount device). Tyto součástky jsou charakteristické svými malými rozměry a tím, že není potřeba jejich vývody protahovat provrtanými otvory. Nezanedbatelnou výhodou je možnost osadit DPS z obou stran součástkami, což snižuje rozměry celé konstrukce.

Při návrhu DPS byl brán zřetel na požadavky pro jejich výrobu. Minimální šířka spoje a šířka mezery mezi spoji je 0,2mm. Nejmenší průměr vrtaného otvoru je 0,3mm. Deska je dvouvrstvá s prokovenými otvory. Pro pozdější a snazší osazení je výhodná povrchová úprava pasivací a nepájivá maska.

Nejdůležitější pro kvalitní návrh DPS je správné rozložení součástek. Konektory pro připojení čidel, elektrospotřebičů, kabelu USB a konektor pro připojení do sítě LAN musí být pro uživatele snadno dostupné. Jsou tedy umístěny na okraji desky. Pro snazší orientaci jsou konektory stejného významu umístěny vedle sebe na jedné straně plošného spoje. Z pohledu z vrchu jsou na horní straně umístěny konektory výstupní, na pravé straně vstupní a na spodní straně jsou konektory pro připojení počítače. Na horní straně DPS jsou mimo konektorů umístěny všechny důležité součástky. Chybí tam pouze ty, které bylo pro jednodušší návrh výhodnější umístit na spodní straně desky.

Základní problematika návrhu DPS se týkala zapojení mikrokontroléru. Ten je orientován tak, aby většina jeho vývodů směřovala přímo k připojeným periferiím. Dosáhlo se tím výrazně menšího křížení vodičů a výsledek působí ucelenějším dojmem. Obě strany desky jsou z vyšší části pokryté zemnícími plochami, které mají sloužit jako stínění a lépe odvádět případné teplo ze spínaného stabilizátoru.

Hotový návrh DPS je uveden v příloze nebo na přiloženém CD.

Osazení a oživení zapojení

Rozmístění součástek bylo nutné přizpůsobit jejich ručnímu osazení bez použití specializované techniky. Při osazování DPS součástkami musíme postupovat tak, abychom si neza-

bránili přístupu ke zbývajícím součástkám. Také vzhledem k tomu, že drahé integrované obvody nejsou zasazeny do patic, ale jsou připájeny přímo k plošnému spoji, tak musíme být ještě více obezřetní.

Při osazování postupujeme tak, že nejdříve zapájíme komponenty zajišťující napájení zařízení. Nejdříve osadíme SMD součástky, posléze stabilizátor a cívku s pouzdrem tavné pojistky. Nožičky stabilizátoru je nutné přibližně 10mm od pouzdra ohnout do pravého úhlu, následně pouzdro přišroubovat připraveným otvorem k desce a až poté jej zapájet. Do držáku vložíme tavnou pojistku a odzkoušíme funkčnost stabilizátoru. Pokud je to možné, použijeme laboratorní zdroj s elektronickým omezením proudu. Napájecí napětí volíme od 10V do 15V a na výstupu stabilizátoru musíme vždy naměřit 5V. Pokud je vše v pořádku osadíme desku stabilizátorem na 3,3V a provedeme stejnou kontrolu.

Další postup osazování již není kritický, doporučuji však nejdříve začít integrovanými obvody, pokračovat SMD součástkami a nakonec zapájet patice, konektory a relé. Velmi doporučuji modul XBee a čtečku RFID osazovat do patic, které je nutné si svépomocí připravit. Rozteč vývodů mají tyto obvody 1,27mm a patice lze tedy vytvořit z patřičné dutinkové lišty, kterou zkrátíme na požadovaný rozměr. Po ukončení pájení zkontrolujeme případné zkraty způsobené chybným pájením a očistíme desku od zbytků tavidel.

Nakonec vyzkoušíme funkčnost hotové ústředny. Při napájení 12V by spotřeba proudu neměla přesáhnout 80mA. Připojíme programátor mikrokontroléru ke konektoru K_{25} a odzkoušíme funkčnost jednotlivých periferií.

6.2.3 Elektronické a mechanické vlastnosti

Ústředna je vybavena celkem třemi konektory k nímž se připojují LCD displej, maticová klávesnice a GSM modul. Tyto moduly jsou k ústředně připojeny přes oboustranný, pozlacený kolíkový konektor dlouhý 20mm. K fixaci modulů k základní desce jsou použity distanční sloupky o stejné délce. Tento druh konstrukce umožňuje vysokou univerzálnost a případnou snadnou výměnu za jiný kus. I když navržený zabezpečovací systém není určen k prodeji, tak jsem jeho konstrukci trochu k tomuto účelu přizpůsobil. V případě, kdy si uživatel nebude přát využít služeb GSM modulu, je možné jim ústřednu nevybavit a zabezpečovací systém nabízet v levnější cenové kategorii.

Rozměry DPS	234mm x 134mm
Nominální napájecí napětí	12V
Rozsah napájecího napětí	10V – 15V
Proudová spotřeba v klidu	180mA
Maximální spotřeba	510mA
Vstupních smyček	8
Výstupních smyček	8
Teplotní rozsah	-25°C – 65°C

Tabulka 6.1: Přehled elektrických a mechanických vlastností ústředny

6.3 Přístupová jednotka a jednotka vstupů a výstupů

6.3.1 Schéma zapojení elektroniky a návrh DPS

U obou přídavných jednotek jsem použil stejná zapojení jako v případě ústředny. Výsledná schémata zapojení elektroniky a DPS jsou uvedeny v příloze nebo na přiloženém CD.

6.3.2 Elektronické a mechanické vlastnosti

	Přístupová jednotka	**Jednotka vstupů a výstupů**
Rozměry DPS	145mm x 109mm	118mm x 94mm
Nominální napájecí napětí	12V	12V
Rozsah napájecího napětí	10V – 15V	10V – 15V
Proudová spotřeba v klidu	55mA	30mA
Maximální spotřeba	415mA	220mA
Vstupních smyček	4	20
Výstupních smyček	4	5
Teplotní rozsah	-25°C – 65°C	-25°C – 65°C

Tabulka 6.2: Přehled elektrických a mechanických vlastností přístupové jednotky a jednotky vstupů a výstupů

6.4 GSM modul

6.4.1 Schéma zapojení elektroniky

Vybraný GSM modem SIM300C (kapitola 3.1.2) je zapojen dle doporučovaného zapojení z katalogového listu výrobce [32]. Pro svoji funkci potřebuje připojení SIM karty a stabilizované napájecí napětí. SIM kartu je vhodné chránit před elektrostatickým výbojem, často označován zkratkou ESD (Electrostatic discharge). Za tímto účelem jsem použil obvod DVIULC6 [5].

Napájecí obvod pro GSM modul je řešen spínaným stabilizátorem LM2576 ve variantě s nastavitelným výstupním napětím. Napětí je nastavitelné v rozsahu od 1,23V až téměř po hodnotu vstupního napětí a jeho regulace se provádí trimrem R_2. GSM modem vyžaduje napájení v rozsahu od 3,4V do 4,5V a výrobce zmiňuje potřebu vyšších nároků na napájecí obvod, protože GSM modem krátkodobě spotřebovává proud až 3A.

Ovládat GSM modem mikrokontrolérem lze pře rozhraní UART. Bohužel přes toto rozhraní není možné modem zapnout. Zapnutí se provádí změnou logické úrovně na pinu PWRKEY, proto je tento pin společně s pinem STATUS vyveden na konektor pro připojení k řídícímu mikrokontroléru.

Výsledné schéma zapojení elektroniky je uvedeno v příloze nebo na přiloženém CD.

6.4.2 Návrh DPS a osazení součástkami

Při návrhu DPS jsem bral zvýšený zřetel na výsledné rozměry. GSM modul se připojuje k ústředně a jeho zbytečně velké rozměry by zvyšovali také velikost ústředny. Podobně jako v předchozích případech je návrh DPS vytvářen se stejnými pravidly, viz 6.2.2.

Pro snadný přístup k SIM kartě, GSM modemu a trimru pro regulaci napájecího napětí jsou tyto komponenty umístěny z horní strany plošného spoje. Na spodní straně je z důvodů minimalizace rozměrů umístěn stabilizátor, který je i zde přišroubován k desce a má nožičky ohnuté do pravého úhlu.

Při osazování opět nejdříve začneme napájecím obvodem a vyzkoušíme jeho funkčnost. Na výstupu bychom měli naměřit napětí, které budeme regulovat trimrem R_2. Nastavíme napětí na 4,5V a budeme pokračovat v dalším osazování. GSM modem je k DPS připojen přes 60ti pinový DIP konektor. SIM karta je vkládána do vyklápěcího konektoru K_2. GSM anténa se připojuje k modemu přes konektor Murata MXTK92 / 50Ω umístěný na spodní straně modemu.

Po kompletním osazení odzkoušíme funkčnost modulu. Uzemněním pinu PWRKEY na dobu nejméně 1,5s zapneme GSM modem a pokud pin STATUS posléze přejde do vysoké logické úrovně, tak se modem skutečně zapnul. Zapnutí také zaregistrujeme zvýšením spotřeby na přibližně 25mA.

Hotový návrh DPS je uveden v příloze nebo na přiloženém CD.

6.4.3 Elektronické a mechanické vlastnosti

Rozměry DPS	78mm x 59mm
Nominální napájecí napětí	12V
Rozsah napájecího napětí	6V – 37V
Proudová spotřeba v klidu	25mA
Proudová spotřeba během hovoru	260mA
Maximální krátkodobá spotřeba	3A
Teplotní rozsah	-25°C – 65°C

Tabulka 6.3: Přehled elektrických a mechanických vlastností GSM modemu

6.5 Záložní zdroj

6.5.1 Schéma zapojení elektroniky

Řešení konstrukce záložního zdroje se skládá ze dvou částí. Z napájecího obvodu stabilizovaného napětí 12V, které je tvořeno spínaným stabilizátorem LM2576 ve variantně nastavitelného výstupního napětí. A z inteligentní nabíječky olověných akumulátorů, která je tvořena obvodem UC3906. Stabilizovaným napětím 12V je napájena cívka relé, které v sepnutém stavu připojuje stabilizované napětí na výstup záložního zdroje. V případě výpadku elektrické energie dojde k odpojení napájení cívky relé, které přepne výstup na záložní akumulátor.

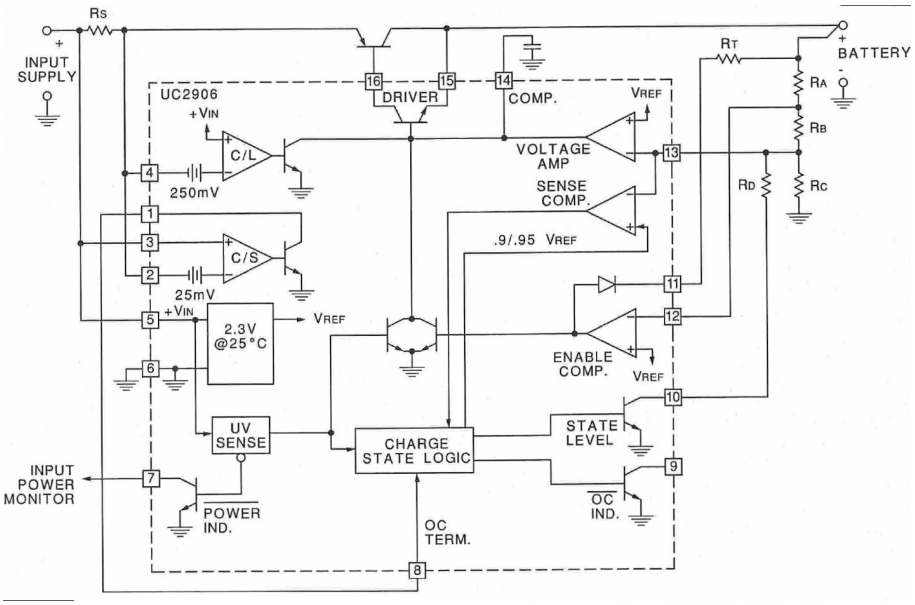
Výsledné schéma zapojení elektroniky je uvedeno v příloze nebo na přiloženém CD.

Inteligentní nabíječka UC3906

Pro konstrukci nabíječky olověných akumulátorů jsem zvolil obvod UC3906 [42]. Dle výrobce obsahuje obvod všechny nezbytné funkce pro optimální kontrolu nabíjení a udržování

maximální životnosti olověných akumulátorů. Při nabíjení monitoruje a přímo ovládá výstupní napětí a proud přes tři samostatné nabíjecí režimy. Nabíjení konstantním proudem, nabíjení konstantním napětím a vyrovnávání samovolného vybíjení. Obvod také zajišťuje ochranu proti přebití akumulátoru. Díky těmto vlastnostem je možné použít nabíječku i v případech, kdy je nutné mít neustále připojený akumulátor.

Blokové schéma a typické zapojení je zobrazeno na obrázku 6.6.



Obrázek 6.6: Blokové schéma a typické zapojení obvodu UC3906 [42]

Ve svém návrhu jsem použil zmíněné doporučené zapojení, které jsem doplnil o ochranu přepólování akumulátoru a indikaci stavu nabíjení. Inspiroval jsem se přitom konstrukcí nabíječky olověných akumulátorů založené na stejném obvodu [33].

6.5.2 Návrh DPS a osazení součástkami

Stejně jako v případech předešlých, tak i při tomto návrhu DPS jsem se snažil o co nejmenší rozměry konstrukce. Výrobce nabíjecího obvodu doporučuje použít 5W výkonový snímací rezistor a také výkonový tranzistor. V mé konstrukci nebylo nezbytně nutné použít tyto výkonové prvky, ale vzhledem k možné výměně akumulátoru za jiný typ, jsem doporučení poslechl.

Při osazování doporučuji začít SMD součástkami, zejména k signalizačním LED diodám a k předřadným rezistorům je velmi špatný přístup při zapájení výkonových prvků. Doporučuji také obvod UC3906 zasadit do příslušné patice. Po kompletním osazení a kontroly DPS provedeme oživení záložního zdroje.

Záložní zdroj napájíme napětím 15V připojeným konektorem K_1, rozsvítí se zelená LED dioda D_4. Trimrem P_1 nastavíme výstupní napětí spínaného stabilizátoru na 12V, které když klesne pod hranici 9V způsobí přepnutí kontaktů relé. Posléze připojíme akumulátor konektorem K_2. Rozsvítí se LED dioda D_6 indikující nabíjení akumulátoru konstantním proudem. Když je akumulátor z větší části nabitý rozsvítí se dioda D_5, která indikuje finální fázi nabíjení. Jakmile obě diody zhasnou, akumulátor je plně nabit a nabíječka přechází do

udržovacího režimu.

6.5.3 Elektronické a mechanické vlastnosti

Rozměry DPS	48mm x 94mm
Nominální napájecí napětí	15V
Rozsah napájecího napětí	14V – 37V
Proudová spotřeba v klidu	10mA
Maximální spotřeba	500mA
Výstupní napětí	12V
Záložní akumulátor	12V / 3,4Ah
Maximální výstupní proud	3A
Teplotní rozsah	-25°C – 65°C

Tabulka 6.4: Přehled elektrických a mechanických vlastností záložního zdroje

6.6 Zhodnocení dosažených výsledků

Po osazení každého modulu jsem provedl ověření jeho hardwarové funkčnosti. Všechna zapojení pracují dle předpokladů a informací od výrobců jednotlivých komponent. U modulu ústředny a tedy i u přístupové jednotky jsem se však setkal s nepřesnými údaji v katalogovém listu RFID čtečky ID12. Výrobce uvádí dosah čtečky 12cm. V mé konstrukci jsem se takové vzdálenosti ani nepřiblížil a čtečka pracuje nejvýše na vzdálenost 3cm. Naštěstí to nijak neovlivňuje funkčnost zařízení. Pouze z bezkontaktní identifikace se tak stala téměř kontaktní.

Nutno také zmínit nekorektní funkčnost záložního zdroje. Při odpojení hlavní elektrické energie se přepíná na záložní akumulátor pomocí elektromagnetického relé. Doba přepnutí by neměla překročit 5ms, avšak i za tak krátkou dobu mikrokontrolér zareaguje na pokles napětí a provede vnitřní reset. Při vhodné softwarové implementaci lze tuto chybu omezit, ale v dalším vývoji bude lépe se zaměřit na důmyslnější způsob přepnutí.

Po ověření funkčnosti hardwaru jsem také ověřil správnou funkci řídících mikrokontrolérů a jejich komunikaci s připojenými periferii. Implementoval jsem jednoduché programy, které měli za účel odhalit případné chybné zapojení. Naštěstí i toto ověření proběhlo bez komplikací a můžu tedy prohlásit hardwarové řešení elektronického zabezpečovacího systému za funkční.

Kapitola 7

Závěr

Ovlivněn bezpečnostní situací v oblasti zabezpečení domácností a rozvíjejícími se moderními technologiemi jsem zvolil poměrně rozsáhlé téma své práce. Detailně jsem se seznámil s aktuálním vývojem majetkové kriminality prováděné vloupáním a se způsoby, jakými lze takovým činům předcházet. Inspirován profesionálními výrobky předních firem vyrábějící elektronické zabezpečovací systémy jsem navrhl a zkonstruoval vlastní takové zařízení.

Při jeho návrhu jsem se opíral o moderní technologie, které usnadní používání zabezpečovacího systému běžným, laickým uživatelům. Zejména bezdrátová komunikace se stala klíčovým prvkem celého návrhu. Přenos poplachu na mobilní telefon přímo majiteli domácnosti nebo do bezpečnostní agentury na pult centrální ochrany zkracuje reakční dobu na probíhající bezpečnostní hrozbu. Zvyšuje se tak pocit bezpečí a jistoty v místě našeho bydliště, což prospívá mimo jiné zdravému životnímu stylu.

Navrhnout takové řešení, z kterého lze některé funkce odebrat stejně snadno, jako nové přidat, bylo od počátku mým záměrem. Realizované zařízení je složeno z pěti modulů, které vytváří jednotný a velice univerzální celek. Řídícím prvkem je modul ústředny, který je navržen tak, aby byl schopen pracovat zcela samostatně. Protože obsahuje všechny důležité periferie, zajišťuje veškerou funkcionalitu systému. Ústřednu je možné připojit k počítači přes rozhraní USB nebo ji připojit do místní sítě LAN a získat tím možnost vzdáleného dohledu a ovládání domácnosti přes internet. Zabezpečovací systém se tak stává prostředkem pro vytvoření inteligentní domácnosti.

I s ohledem na seniory, kteří často mají problém naučit se ovládat pro nás jednoduchá zařízení, jsem navrhl ovládání systému pomocí přístupové jednotky. Jejím umístěním ke vchodovým dveřím bude uživatel při odchodu schopen domácnost snadno zabezpečit a stejně snadno při příchodu zabezpečení vypnout. Aby ho tato činnost příliš neomezovala, tak je přístupová jednotka vybavena RFID čtečkou pro bezkontaktní identifikaci. Zmíněný úkol provedeme pouhým přiložením patřičné identifikační karty nebo přívěšku na klíče. Nechci však uživatele nijak omezovat, a proto přístupová jednotka obsahuje numerickou klávesnici pro zadání soukromého hesla nebo bude možné systém ovládat přes mobilní telefon formou SMS zpráv.

Abychom mohli vždy správně a přesně reagovat na bezpečnostní hrozbu, tak musí zabezpečovací sytém být schopný rozlišit od sebe jednotlivá čidla. Ve větších domácnostech se můžeme setkat s potřebou připojit vysoký počet čidel, a proto jsem navrhl jednotku vstupů a výstupů. Ta se stará o rozšíření počtu připojitelných čidel a elektrospotřebičů bez nutnosti se omezovat v našich požadavcích.

Komunikace mezi jednotlivými částmi systému je realizována bezdrátově za použití protokolu ZigBee postaveného nad standardem IEEE 802.15.4. Právě fakt, že je navržené

zařízení bezdrátové umožňuje jeho velice snadnou instalaci nebo případnou změnu. Rozšířit systém o zcela nový modul (například pro měření a regulaci teploty v místnosti) je díky tomu také velice jednoduché.

Proti nebezpečí výpadku elektrické energie je systém napájen záložním zdrojem tvořeným inteligentní nabíječkou olověných akumulátorů, která se stará o maximální životnost a nabití vloženého akumulátoru.

Realizace mé práce se skládala z několika dílčích kroků. Nejdříve jsem navrhl způsob, jakým bude zařízení pracovat. Je rozděleno na pět samostatných částí. Část ústředny, GSM modulu, jednotky přístupu, jednotky vstupů a výstupů a záložního zdroje. Každá část se skládala z výběru vhodných součástek, které jsou běžně dostupné v maloobchodní síti elektrotechnických prodejen. S ohledem na doporučení výrobců jednotlivých součástek jsem navrhl schéma zapojení elektroniky. Pro vlastní realizaci byl velmi důležitým krokem návrh desek plošných spojů, které se posléze vyrobili u specializované firmy. Součástky jsem objednal a ručně jimi osadil vyrobené plošné spoje. Nakonec jsem provedl ověření funkčnosti zapojení pomocí krátkých, jednoúčelových programů pro mikrokontroléry.

Aktuálně je práce ve stavu kompletně funkční hardwarové realizace. V dalším vývoji je nutné se zaměřit na softwarovou implementaci pro mikrokontroléry a vytvořit vhodné uživatelské a administrační rozhraní pro počítač. Těmto úkolům bych se chtěl věnovat v navazujícím studiu, a protože realizované zařízení zůstane na fakultě informatiky, tak se nabízí případná spolupráce se studenty, kteří se zajímají o zabezpečovací techniku.

Vložené přílohy obsahují výkresy elektrotechnických schémat, seznam použitých součástek a návrhy plošných spojů včetně jejich osazení. Nechybí ani fotografie hotového zařízení. Vše obsahuje také přiložené CD.

Literatura

[1] Atmel: XMEGA MANUAL. 2010, [Online; navštíveno 11.05.2010].
URL http://www.atmel.com/dyn/resources/prod_documents/doc8077.pdf

[2] Axelson, J.: *Embedded Ethernet and Internet Complete*. Lakeview Research LLC, 2003, iSBN 1-931448-00-0.

[3] Bílek, J.: Síťové modely, základy IP adresování. Cisco Akademie, FIT VUT v Brně, 2008, [Online; navštíveno 11.05.2010].
URL http://netacad.fit.vutbr.cz/texty/case_study_cc3/icnd1-1_2.pdf

[4] Digi International: XBee & XBee-PRO 802.15.4 OEM RF Modules. 2010, [Online; navštíveno 09.05.2010].
URL http://www.digi.com/products/wireless/point-multipoint/xbee-series1-module.jsp

[5] DVIULC6-4SC6 datasheet: 2010, [Online; navštíveno 11.05.2010].
URL http://www.st.com/stonline/products/literature/ds/11599.pdf

[6] Eady, F.: *Hands-On ZigBee: Implementing 802.15.4 with Microcontrollers*. Elsevier Inc., 2007, iSBN 0-1237-0887-7.

[7] ENC28J60 Data Sheet - Stand-Alone Ethernet Controller with SPI Interface: [Online; navštíveno 11.05.2010].
URL http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf

[8] FT2232D dual USB to serial UART/FIFO IC datasheet: 2009, [Online; navštíveno 11.05.2010].
URL http://www.ftdichip.com/Documents/DataSheets/DS_FT2232D.pdf

[9] FTDI Ltd: Software application development D2XX programmers guide. 2010, [Online; navštíveno 11.05.2010].
URL http://www.ftdichip.com/Documents/ProgramGuides/D2XX_Programmer's_Guide(FT_000071).pdf

[10] GSM Association: Brief History of GSM & the GSMA. 2010, [Online; navštíveno 06.05.2010].
URL http://www.gsmworld.com/about-us/history.htm

[11] Hankovec, D.: Protokol Wiegand a řešení jeho čtení procesorem. 2010, [Online; navštíveno 10.05.2010].
URL http://www.dhservis.cz/dalsi_1/wiegand.htm

[12] Hasičský záchranný sbor ČR : Vyhláška č.23/2008. 2009, [Online; navštíveno 05.05.2010].
URL www.hzscr.cz/soubor/vyhlaska-23-2008-pdf-578562.aspx

[13] Hasičský záchranný sbor ČR : Statistická ročenka 2009. 2010, [Online; navštíveno 05.05.2010].
URL http://www.hzscr.cz/soubor/rocenka-2009-pdf.aspx

[14] ID Innovations: 2010, [Online; navštíveno 10.05.2010].
URL http://www.id-innovations.com/Modules(nonwrite).htm

[15] Jablotron alarms: 2010, [Online; navštíveno 23.02.2010].
URL http://zabezpecovaci-technika.jablotron.cz

[16] Kainka, B.: *USB - měření, řízení a regulace pomocí sběrnice USB*. BEN - technická literatura, 2002, iSBN 80-7300-073-3.

[17] Koton J., Číka P., Křivánek V.: Standard nízkorychlostní bezdrátové komunikace ZigBee. 2006, [Online; navštíveno 08.05.2010].
URL http://access.feld.cvut.cz/view.php?cisloclanku=2006032001

[18] LF33CDT datasheet: 2010, [Online; navštíveno 11.05.2010].
URL http://www.st.com/stonline/books/pdf/docs/2574.pdf

[19] LM2576 datasheet: 2010, [Online; navštíveno 11.05.2010].
URL http://www.onsemi.com/pub_link/Collateral/LM2576-D.PDF

[20] Lukáš, V.: RFID - technologie pro internet věcí. 2009, [Online; navštíveno 10.05.2010].
URL http://access.feld.cvut.cz/view.php?cisloclanku=2009020001

[21] Ministerstvo vnitra ČR: Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2008 (ve srovnání s rokem 2007). 2009, [Online; navštíveno 11.02.2010].
URL http://www.mvcr.cz/clanek/bezpecnostni-situace-dokumenty.aspx

[22] Navos security: Připojení na PCO. 2009, [Online; navštíveno 04.05.2010].
URL http://www.navos.cz/str2.php

[23] Novinky.cz: Bezpečnostní fólie na oknech ochrání skla před uličníky a zloději. 2009, [Online; navštíveno 22.04.2010].
URL http://www.novinky.cz/bydleni/tipy-a-trendy/158284-bezpecnostni-folie-na-oknech-ochrani-skla-pred-ulicniky-a-zlodeji.html

[24] NXP Semiconductors: Level shifting techniques in I2C-bus design. 2007, [Online; navštíveno 11.05.2010].
URL http://www.nxp.com/documents/application_note/AN10441.pdf

[25] P-mont, Šlahora: Kovové ploty. 2007, [Online; navštíveno 22.04.2010].
URL http://www.p-mont.cz/kovove-ploty.aspx

[26] Paradox security systems: 2010, [Online; navštíveno 23.02.2010].
URL http://www.paradox.com

[27] Paret, D.: *RFID and contactless smart card applications*. John Wiley & Sons Ltd, 2005, iSBN 0-470-01195-5.

[28] PulseJack 1x1 Tab-Down RJ45: [Online; navštíveno 11.05.2010].
URL http://www.soselectronic.com/a_info/resource/a/pdf/j0006.pdf

[29] RFC INDEX: [Online; navštíveno 11.05.2010].
URL http://tools.ietf.org/rfc/

[30] Richtr, T.: Technologie pro mobilní komunikaci. 2003, [Online; navštíveno 06.05.2010].
URL http://tomas.richtr.cz/mobil/gsm-strukt.htm

[31] SHERLOCK BOHEMIA, s.r.o.: Protipožární bezpečnostní dveře - Excelent - F6/4 Nucleo. 2007, [Online; navštíveno 24.04.2010].
URL http://www.sherlock.cz/.442.html

[32] SIMCom Ltd.: SIM300C/SIM340C. 2008, [Online; navštíveno 07.05.2010].
URL
http://www.sim.com/wm/wm/html/en/wms/EDGEModule/ProductDetail.aspx?id=4

[33] Slánský, M.: Inteligentní nabíječka Pb akumulátorů. 2006, [Online; navštíveno 11.05.2010].
URL http://hw.cz/Teorie-a-praxe/Konstrukce/ART1685

[34] SOS electronic s.r.o.: Moduly RFID. 2010, [Online; navštíveno 10.05.2010].
URL http://www.soselectronic.cz/?str=12\&code=D3010\&level=4

[35] SPŠ sdělovací techniky, Panská 3, Praha 1: Spínaný stabilizátor napětí. 2008, [Online; navštíveno 11.05.2010].
URL http://panwiki.panska.cz/index.php/Spínaný_stabilizátor_napětí

[36] Stanislav Křeček a kol.: *Příručka zabezpečovací techniky*. Blatenská tiskárna, 2006, iSBN 80-902938-2-4.

[37] Statutární město Brno - Městská policie Brno: Používání nápisu „STOP“ a Jednotka operativního zásahu. 2007, [Online; navštíveno 04.05.2010].
URL http://www.mpb.cz/verejne-informace/poskytovane-informace-2007/pouzivani-napisu-stop-a-jednotka-operativniho-zasahu

[38] Statutární město Brno - Městská policie Brno: Výstupy z projektu prevence kriminality „ONI“, který byl realizován v roce 2008. 2009, [Online; navštíveno 11.02.2010].
URL http://www.mpb.cz/fileadmin/user_upload/Prevence/ONI/VYHODNOCENI_PROJEKTU_ONI_-_WEB.pdf

[39] Statutární město Brno - Městská policie Brno: Centrum tísňového signálu. 2010, [Online; navštíveno 11.02.2010].
URL
http://www.mpb.cz/odbor-prevence/pro-seniory/centrum-tisnoveho-signalu

[40] Telit: GC864-QUAD-PY. 2010, [Online; navštíveno 07.05.2010].
URL
http://www.telit.com/en/products/gsm-gprs.php?p_id=12\&p_ac=show\&p=12

[41] TME Czech Republic s.r.o.: [Online; navštíveno 07.05.2010].
URL http://www.tme.eu/cz/katalog/artykuly.phtml?search=gprs

[42] UC3906 datasheet: 1996, [Online; navštíveno 11.05.2010].
URL http://focus.ti.com/lit/ds/symlink/uc3906.pdf

[43] Wikipedie: Fresnel lens. 2010, [Online; navštíveno 04.05.2010].
URL http://en.wikipedia.org/wiki/Fresnel_lens

[44] Wikipedie: Passive infrared sensor. 2010, [Online; navštíveno 04.05.2010].
URL http://en.wikipedia.org/wiki/Passive_infrared_sensor

[45] Wikipedie: Universal Serial Bus. 2010, [Online; navštíveno 11.05.2010].
URL http://en.wikipedia.org/wiki/Universal_Serial_Bus

[46] Zbyněk Hloušek - zabezpečovací systémy: Magnetické kontakty. 2007, [Online; navštíveno 22.04.2010].
URL http://www.zabezpeceni-domu.cz

[47] Český statistický úřad: Mobilní telefonní síť. 2010, [Online; navštíveno 06.05.2010].
URL http://www.czso.cz/csu/redakce.nsf/i/mobilni_telefonni_sit

[48] ČIP plus s.r.o.: Jak nainstalovat požární hlásič. 2010, [Online; navštíveno 05.05.2010].
URL http://www.hlasic-pozaru.cz/pozarni_hlasice/jak_nainstalovat_pozarni_hlasic.php

Seznam příloh

A Fotografie realizovaného projektu.

B Seznam použitých součástek.

C Schéma zapojení elektroniky jednotlivých modulů.

D Desky plošných spojů a jejich osazení.

E Datový nosič se zdrojovými soubory a podklady pro konstrukci. Podrobný obsah je vypsán v souboru README v kořenovém adresáři CD.